

Jahresbericht

der

Deutschen Mathematiker-Vereinigung.

Vierter Band.

1894—95.

Enthaltend die Chronik der Vereinigung für die Jahre 1894 und 1895, kurze Berichte über die auf den Versammlungen in Wien und Lübeck gehaltenen Vorträge, sowie einen ausführlichen

Bericht über die Theorie der algebraischen Zahlkörper,

von **David Hilbert** in Göttingen.

Herausgegeben im Auftrage des Vorstandes

von

A. Wangerin
in Halle a. S.

A. Gutzmer
in Halle a. S.

Berlin.
Druck und Verlag von Georg Reimer.
1897.

Inhalt.

I. Chronik der Deutschen Mathematiker-Vereinigung.

II. Bericht über die wissenschaftlichen Sitzungen zu Wien.

III. Bericht über die wissenschaftlichen Sitzungen zu Lübeck.

IV. Die Theorie der algebraischen Zahlkörper.

Chronik

der

Deutschen Mathematiker-Vereinigung.

Bericht über die Jahresversammlung
zu Wien.*)

Am 24. bis 28. September 1894.

Nachdem im Vorjahre die Mitglieder der Deutschen Mathematiker-Vereinigung, um die Vorbereitung und Aufstellung der damals veranstalteten Mathematischen Ausstellung zu ermöglichen, getrennt von der in Nürnberg tagenden Naturforscher-Versammlung in München zusammengekommen waren, hatte sich in diesem Jahre die Deutsche Mathematiker-Vereinigung mit der ersten Abteilung für Mathematik der Gesellschaft Deutscher Naturforscher und Aerzte wieder vereinigt, und es hatten sich 56 Mathematiker aus deutschen und österreichischen Landen mit einigen Gästen aus Russland und aus Schweden in den prächtigen Räumen der Wiener Universität zusammengefunden.

Die wissenschaftlichen Vorträge wurden eingeleitet durch die Begrüssungsreden der Herren v. Escherich und Gordan. Der erstere bewillkommte als einführender Vorsitzender des Wiener Comité's die Erschienenen und widmete hierauf herzliche Worte des Andenkens seinem jüngst verstorbenen Collegen Emil Weyr; der Vorsitzende der Deutschen Mathematiker-Vereinigung P. Gordan kennzeichnete eingehend Wirken und Ziele der Vereinigung und gab kurzen Bericht von der Tätigkeit derselben im verflossenen Jahre.

Wir stellen im Folgenden die Liste der in den Sitzungen vom 24. bis 28. September gehaltenen Vorträge zusammen und verweisen bezüglich derselben noch auf die im zweiten Teile enthaltenen Referate.

---

*) Erstattet von W. Dyck.

1. Wassiljef (Kasan). Lobatschefskij's Ansichten über die Theorie der Parallellinien vor dem Jahre 1826.
2. Königsberger (Heidelberg). Zur Theorie der partiellen Differentialgleichungen.
3. Klein (Göttingen). Ueber lineare homogene Differentialgleichungen zweiter Ordnung zwischen zwei Variabeln.
4. Gordan (Erlangen). Ueber das Zerfallen von Curven in gerade Linien.
5. F. Meyer (Clausthal). Die Resultantenbildungen der Trigonometrie.
6. Dyck (München). Zur Theorie d. Charakteristiken v. Functionensystemen.
7. Stäckel (Halle). Ueber Anwendungen der Lie'schen Gruppentheorie auf die Dynamik.
8. Mandl (Prossnitz). Ueber ein Kriterium für die Irreducibilität ganzer Functionen.
9. Czuber (Wien). Ueber einen symbolischen Calcul auf Trägern vom Geschlechte eins.
10. Simony (Wien). Ueber die Einführung topologischer Gattungsbegriffe in die Lehre von den Verschlingungen.
11. Lerch (Prag). Ueber ein bei einer Cauchy'schen Transformation der elliptischen Elementarfunction 3. Ordnung auftretendes Integral.
12. Kohn (Wien). Ueber die Erweiterung eines Grundbegriffes der Geometrie der Lage.
13. Wirtinger (Wien). Ueber den Zusammenhang der Kummer'schen Fläche mit der projectiven Erzeugung der ebenen Curven 4. Ordnung mit Doppelpunkt.
14. Zindler (Wien). Ueber eine neue Erzeugungsweise des linearen Complexes durch zweimalige Rotation.
15. J. Schmidt (Budapest). Bemerkungen über Bolyai's Tentamen.
16. Zsigmondy (Wien). Ueber Congruenzen, welche in Bezug auf einen Primzahlmodul keine Wurzeln haben.
17. Wälsch (Prag). Ueber eine Behandlungsweise d. Flächen dritter Ordnung.
18. Gutzmer (Berlin). Neue Herleitung des Kirchhoff'schen Ausdruckes für das Huygens'sche Princip.
19. Landsberg (Heidelberg). Zur Theorie der algebraischen Zahlen.
20. Tauber (Wien). Ueber die Werte einer analytischen Function längs einer Kreislinie.
21. Kiepert (Hannover). Ueber die mathematische Ausbildung der Versicherungstechniker.
22. Krause (Dresden). Zur Transformationstheorie d. elliptischen Functionen.
23. Wangerin (Halle). Zur Geschichte der Theorie der conformen Abbildung.

In der 2. allgemeinen Sitzung der Naturforscher-Versammlung hielt Herr F. Klein einen Vortrag über: Riemann und seine Bedeutung für die Entwickelung der modernen Mathematik, welcher im zweiten Teile dieses Jahresberichts zum Abdruck gelangt.

Im Laufe der Wiener Versammlung wurden die Themata für eine Reihe von wissenschaftlichen Referaten eingehend besprochen, deren Ausführung für die folgenden Jahre in Aussicht genommen ist.

Neben dem von den Herren Hilbert und Minkowski bearbei-

teten Referate über Zahlentheorie und den schon im Vorjahre erwähnten Berichten Pringsheim's über die Lehre von den unendlichen Reihen und E. Kötter's über synthetische Geometrie wurden besprochen:

1. ein Referat über Abel'sche Functionen von Herrn Wirtinger;

2. ein Referat über Wahrscheinlichkeitsrechnung von Herrn Czuber.

3. Den Plan eines Berichtes über Differentialgeometrie gab Herr Stäckel;

4. einen solchen über Liniengeometrie legte Herr Wälsch vor.

5. Der Vortrag des Herrn Kiepert „Ueber die mathematische Ausbildung der Versicherungstechniker" regte die Frage an, ob es nicht zweckmässig wäre, für eine der folgenden Versammlungen einen Bericht „Ueber Einrichtung und Ausgestaltung von Vorlesungen in der angewandten Mathematik" zu veranlassen, bei welchem insbesondere die Möglichkeit des Ineinandergreifens der praktischen Interessen der Techniker und der Juristen mit den Anforderungen der Theorie ins Auge zu fassen wäre.

Des weiteren wurde der Plan der Herausgabe eines mathematischen Lexikons eingehend besprochen.

Die Versammlung erkannte die hohe Wichtigkeit eines derartigen Unternehmens an, dessen materielle Durchführung als eine geeignete Aufgabe für das im Jahre 1893 ins Leben gerufene Akademien-Cartell erschien. Im Hinblick darauf beauftragte die Versammlung ihre den Akademien bez. gelehrten Gesellschaften zu Göttingen, Leipzig, München und Wien angehörenden Mitglieder, die Unterstützung des Unternehmens ihren Akademien in Vorschlag zu bringen.

Herr Lampe (Berlin) berichtete noch über einen von einer Gruppe französischer Mathematiker in Aussicht genommenen internationalen Mathematikercongress. Die Vereinigung sprach im Principe ihre Sympathie für diesen Plan aus und beauftragte ihren Vorstand, gegebenen Falles Schritte für eine würdige Vertretung der deutschen Mathematiker zu thun.

Im Laufe der Verhandlungen kam der Wunsch zum Ausdrucke, dass bei den künftigen Versammlungen der Mathematiker-Vereinigung und der Gesellschaft Deutscher Naturforscher und Aerzte eine gemeinschaftliche Sitzung mit den Physikern in Aussicht genommen und dabei ein Programm für gemeinschaftliche Vorträge und Verhandlungen vorbereitet werde.

Geschäftlicher Bericht.

1. Die geschäftliche Sitzung der Vereinigung fand während der Wiener Versammlung am 28. September unter dem Vorsitze von Herrn Gordan statt. Hierbei erstattete Herr Dyck als Schrift- und Kassenführer vorläufigen Bericht über den Stand der Kasse. Wir geben untenstehend die Zusammenstellung der Einnahmen und Ausgaben nach dem Stande vom 1. Januar 1895. In dieser Zusammenstellung ist der von der Mathematischen Ausstellung zu München (vergl. Jahresbericht III pg. 10) herrührende Restbetrag dieses Unternehmens nicht mehr aufgeführt. Derselbe wurde durch einstimmigen Vorstandsbeschluss vom 5. Januar 1895 zusammt dem Verlagsrechte über die bei Gelegenheit der Ausstellung erschienenen Schriften dem Leiter jener Ausstellung, Herrn Dyck, als Ehrengabe überwiesen.

2. An Stelle der aus dem Vorstande statutengemäss ausscheidenden Herren Dyck, Lampe und Reye wurden in der Sitzung vom 28. September 1894 neu gewählt die Herren Brill, Gutzmer, Wangerin, welche sämmtlich die auf sie gefallene Wahl annahmen. Innerhalb des Vorstandes wurde für das Jahr 1895 Herr H. Weber zum Vorsitzenden, Herr A. Gutzmer zum Schriftführer gewählt und als Redactions-Commission für den Jahresbericht die Herren Gutzmer und Wangerin bestimmt.

Kassenbericht für das Jahr 1894.

Einnahmen.	M.	Pf.	Ausgaben.	M.	Pf.
Cassarest vom Vorjahr 1893	66	34	Drucksachen	27	—
Beiträge der Mitglieder:			Buchbinder u. Verschiedenes	43	—
Nachträge pro 1893 . .	76	01	Postporti	53	08
Beiträge pro 1894 . . .	266	41	Honorare für die Referate im Jahresbericht . . .	969	50
Vorauszahlung pro 1895	39	99	Summa der Ausgaben	1092	58
Ablösung d. Jahresbeiträge	329	87	Cassarest pro 1895 . . .	908	59
Von der Verlagshandlung von G. Reimer für den 3. Jahresbericht 93/94 .	1177	50			
Erlös aus dem Verkauf des Dissertationenverzeichn.	18	05			
Zins aus den 900 M. 3% Reichsanleihe	27	—			
Summa der Einnahmen	2001	17	Summa	2001	17

W. Dyck, als Kassenführer. K. Döhlemann, A. Pringsheim als Revisoren.

Bericht über die Jahresversammlung
zu Lübeck.

16.—20. September 1895.

In Uebereinstimmung mit den Statuten der Deutschen Mathematiker-Vereinigung fand die diesjährige Jahresversammlung in Gemeinschaft mit der „I. Abteilung für Mathematik und Astronomie der Gesellschaft Deutscher Naturforscher und Aerzte“ statt, und es waren der Einladung des Vorstandes 43 Mathematiker aus Deutschland und aus fremden Staaten nach der alten gastlichen Hansastadt Lübeck gefolgt.

Als Einführender der Abteilung für Mathematik und Astronomie hiess Herr W. Godt die Erschienenen bei Eröffnung der Sitzungen willkommen; anstelle des am Erscheinen verhinderten Herrn H. Weber, des derzeitigen Vorsitzenden der Deutschen Mathematiker-Vereinigung, begrüsste Herr P. Gordan insbesondere deren Mitglieder und eröffnete die diesjährigen wissenschaftlichen Sitzungen der Vereinigung mit einer Kennzeichnung der Aufgaben der letzteren.

Die Reihe der Vorträge wurde eröffnet durch die Herren Hilbert und Minkowski, welche sich über die in ihrem Bericht über den gegenwärtigen Stand der Zahlentheorie zur Behandlung kommende Materie und deren Disposition eingehend äusserten. Sodann gab Herr E. Kötter eine ausführliche Darlegung über Plan und Inhalt seines Referats über die Entwickelung der synthetischen Geometrie. Es ist mit Bestimmtheit zu hoffen, dass beide Berichte im Jahre 1896 gedruckt bezw. druckfertig vorliegen werden.

Die folgende Zusammenstellung umfasst die Titel der übrigen Vorträge; die eingegangenen Referate über dieselben sind im dritten Teile dieses Jahresberichts enthalten:

1. Frege (Jena). Ueber die Begriffsschrift des Herrn Peano und meine eigene.
2. Wangerin (Halle a. S.). Ueber Franz Neumann's mathematische Arbeiten.
3. Lampe (Berlin). Ueber die Herstellung eines allgemeinen bibliographischen Repertoriums.
4. Heffter (Giessen). Ueber gemeinsame Teiler und gemeinsame Vielfache linearer Differentialausdrücke.
5. Voss (Würzburg). Ueber infinitesimale Flächendeformationen.
6. Pokrowsky (Kiew). Ueber die hyperelliptischen Functionen von zwei Argumenten.
7. Souslow (Kiew). Ueber eine continuirliche Gruppe von Darboux-schen Rotationen.
8. Joukowsky (Moskau). Geometrische Interpretation des von Sophie Kowalevski behandelten Falles der Bewegung eines schweren starren Körpers um einen festen Punkt.
9. Fricke (Braunschweig). Die Discontinuitätsbereiche der Gruppen reeller linearer Substitutionen einer complexen Veränderlichen.
10. Klein (Göttingen). Zur Theorie der gewöhnlichen Kettenbrüche.
11. Gordan (Erlangen). Der Pascal'sche Satz.
12. Schubert (Hamburg). Ueber correlative Verwandtschaft in n Dimensionen.
13. Gutzmer (Berlin). Ueber gewisse lineare Differentialgleichungen.
14. Godt (Lübeck). Ueber den Feuerbach'schen Kreis und die Steiner-sche Curve vierter Ordnung und dritter Klasse.
15. Kohn (Wien). Zur geometrischen Deutung der homogenen Coordinaten.
16. London (Breslau). Ueber cubische Constructionen.
17. Meyer (Clausthal). Ueber eine Abhandlung des Herrn L. Schendel: Ueber unendliche Reihen und Producte.
18. Gutzmer (Berlin). Ueber eine Arbeit des Herrn Schoute: Ueber eine gewisse Einhüllende.

Gemäss dem auf der vorjährigen Versammlung geäusserten Wunsche fand in Lübeck auch eine gemeinschaftliche Sitzung mit den Physikern statt; ausser dem Referate des Herrn Helm (Dresden) „über den derzeitigen Zustand der Energetik", durch welches eine mehrstündige, sehr eingehende Debatte über diesen Gegenstand eingeleitet und veranlasst wurde, das aber unter den Referaten des III. Teiles dieses Berichts nicht berücksichtigt werden konnte, wurden noch folgende wissenschaftliche Mitteilungen gemacht:

19. Schütz (Göttingen). Ueber eine verwandte Gruppe thermodynamischer, elektrodynamischer und astrophysikalischer Thatsachen.
20. Sommerfeld (Göttingen). Diffractionsprobleme in exacter Behandlung.

Bei der Besprechung der bereits früher in Aussicht genommenen Referate über grössere Gebiete wurde es als wünschenswert bezeichnet, den von Herrn Wirtinger übernommenen Bericht über Abel'sche Functionen bis nach dem Erscheinen des III. Bandes der Gesammelten Werke des Herrn Weierstrass und der Vorlesungen desselben über die Theorie der Abel'schen Transcendenten zu vertagen. Dagegen wurde die Theorie der Functionen eines reellen Arguments als ein Gebiet bezeichnet, welches für ein Referat ins Auge zu fassen sei.

Wie auf der Jahresversammlung zu München im Jahre 1892 entspann sich auf Anregung von Herrn Brill auch im Laufe der diesjährigen Sitzungen eine Discussion über die Aufgaben des mathematischen Unterrichts an deutschen Hochschulen (einschliesslich der Technischen Hochschulen), und es wurden die Herren Brill und Klein gebeten, diesen Gegenstand im Auge zu behalten und auf einer der nächsten Jahresversammlungen zur Verhandlung zu bringen.

Der im vorigen Jahre (vgl. den vorstehenden Bericht über die Wiener Versammlung) erörterte Plan der Herausgabe eines mathematischen Lexikons hat inzwischen festere Gestalt gewonnen; seine Durchführung erscheint durch die in Aussicht stehende materielle Unterstützung der Akademien zu Göttingen, München und Wien und infolge des Entgegenkommens der Verlagsbuchhandlung von B. G. Teubner in Leipzig gesichert. Eine aus Mitgliedern der genannten Akademien bestehende Commission hat in dem Wunsche, enge Beziehung zu der Deutschen Mathematiker-Vereinigung zu behalten, den derzeitigen Vorsitzenden derselben, Herrn H. Weber in Strassburg, cooptirt, welcher der Vereinigung fortlaufende Mitteilungen über den jeweiligen Stand der Sache machen wird.

In Bezug auf den geplanten internationalen Mathematikercongress konnte die Versammlung nur die im Vorjahre zum Ausdruck gekommene Meinung dahin präcisiren, dass die Vereinigung einem derartigen Unternehmen sympathisch gegenüberstehe, jedoch nicht die Initiative ergreifen wolle.

Aus Anlass eines Briefes des Herrn P. Molenbroek-Haag, in welchem die Gründung einer internationalen Gesellschaft zur Förderung der Vectorentheorien (Hamilton'sche Quaternionentheorie, Grassmannsche Ausdehnungslehre u. s. w.) angeregt wird, sprach die Versammlung ihre Bedenken gegen die Stiftung eines derartigen Vereines aus, der lediglich den Zweck hat, einen sehr eng begrenzten Teil des mathematischen Wissens zu fördern.

Die Versammlung beschloss ferner, Herrn Weierstrass an seinem

achtzigsten Geburtstage (31. October 1895) die Glückwünsche der Vereinigung in Form einer kunstvoll ausgestatteten Adresse darzubringen. Der aus der Feder des Herrn Weber stammende Entwurf der letzteren wurde genehmigt, und es wurden die Herren Brill, Wangerin und Gutzmer mit der Ueberreichung der Adresse betraut. Der Wortlaut der Adresse ist in die Chronik aufgenommen worden.

Schliesslich kam der Umstand zur Sprache, dass infolge der jetzt üblichen drei allgemeinen Sitzungen der Naturforscherversammlungen die Zeit für die fachwissenschaftlichen Sitzungen der Abteilungen nicht ausreichend sei, und es wurde daher Herr Klein beauftragt, im Vorstande der Gesellschaft Deutscher Naturforscher und Aerzte dahin zu wirken, dass eine der allgemeinen Sitzungen fortfällt, um so Zeit für gemeinsame Sitzungen verwandter Abteilungen zu gewinnen, welche durch den genannten Vorstand mit Hülfe des wissenschaftlichen Ausschusses vorzubereiten sind.

Geschäftlicher Bericht.

1. Während der Lübecker Versammlung fand unter dem Vorsitze des Herrn P. Gordan eine geschäftliche Sitzung am 19. September statt, in welcher der Schrift- und Kassenführer Herr Gutzmer einen Bericht über die Vermögenslage und über die erfreuliche Zunahme der Mitgliederzahl erstattete. Nebenstehend findet sich eine Uebersicht über die Einnahmen und Ausgaben nach dem Stande vom 1. December 1895, dem Zeitpunkte der Drucklegung dieses Berichtes.

2. Zu Kassenrevisoren wurden die Herren E. Lampe und E. Kötter gewählt. Um der Forderung des § 3 der Statuten zu entsprechen, dass alljährlich zwei Mitglieder aus dem Vorstande ausscheiden und durch Neuwahl ersetzt werden sollen, wurde bestimmt, dass ausser dem Ende 1895 turnusmässig ausscheidenden Herrn P. Gordan auch Herr A. Gutzmer zu diesem Zeitpunkte ausscheide; die darauf vorgenommenen Wahlen ergaben das Resultat, dass Herr F. Klein neu gewählt und Herr A. Gutzmer wiedergewählt wurde. Der Vorstand der Vereinigung besteht also für das Jahr 1896 aus folgenden Herren, wobei der Uebersichtlichkeit wegen durch die in Klammern beigefügten Zahlen das Jahr bezeichnet worden ist, an dessen Ende der Betreffende statutengemäss auszuscheiden hat: H. Weber (96), G. von Escherich (96), A. Brill (97), A. Wangerin (97), F. Klein (98), A. Gutzmer (98).

3. Die Wahlen innerhalb des Vorstandes haben für das Jahr 1896 folgendes Resultat ergeben: A. Brill, Vorsitzender; A. Gutzmer, Schrift- und Kassenführer; A. Wangerin und A. Gutzmer, Redactionscommission für den Jahresbericht.

4. In Betreff des Jahresberichtes der Vereinigung wurde beschlossen, den Druck desselben, der bisher aus zeitweiligem Mangel an grösseren Referaten unterblieben war, nunmehr ungesäumt von Statten gehen zu lassen, und die Berichte über die Wiener und Lübecker Versammlungen zu einem Bande zu vereinigen.

5. Die zur Ueberreichung der Glückwunsch-Adresse der Vereinigung für Herrn Weierstrass gewählte Abordnung hat sich ihres Auftrages am 31. October 1895 entledigt. Herr Weierstrass sprach der Vereinigung in freundlichen Worten seinen Dank aus.

5. Die nächste Zusammenkunft der Vereinigung wird in Gemeinschaft mit der Jahresversammlung der Gesellschaft Deutscher Naturforscher und Aerzte abgehalten werden; nach dem in Lübeck gefassten Beschluss wird dieselbe 1896 in Frankfurt a. M. stattfinden.

Kassenbericht.

Nach dem Stande vom 1. December 1895.

Einnahmen.	M.	Pf.	Ausgaben.	M.	Pf
Kassenrest von 1894 . . .	908	59	Drucksachen	34	—
Jahresbeiträge der Mitglieder:			Verschiedenes (Papier etc.)	7	—
1 Nachtrag für 1892 . . .	2	05	Postporti	47	62
4 Nachträge für 1893 . . .	8	—	Adresse für Herrn Weierstrass	92	—
7 Nachträge für 1894 . . .	14	—	900 M. 3% Reichsanleihe à 98,20	894	35
92 Beiträge für 1895 . . .	184	79	Baarbestand	492	96
13 Vorauszahlungen für 1896	25	50			
3 Vorauszahlungen f. 1897	6	—			
1 Vorauszahlung für 1898	2	—			
13 Ablösungen der Jahresbeiträge	390	—			
½ Jahr Zinsen von 1800 M. 3% Reichsanleihe. . . .	27	—			
Summe	1567	93	Summe	1567	93

Gegenwärtiger Kassenstand:

Nom. 1800 M. 3% Reichsanleihe, im Ankaufswert von M. 1687.90
und baarer Kassenbestand M. 492.96.

A. Gutzmer, als Kassenführer.

E. Lampe, E. Kötter, als Revisoren.

Mitglieder-Verzeichnis

der Deutschen Mathematiker-Vereinigung

nach dem Stande vom 1. December 1895.

Abbe, C., Meteorological Institute, Washington.
Ackermann-Teubner, Verlagsbuchhändler, Leipzig.
Adami, Reallehrer an der Realschule, Bayreuth.
Amthor, A., Hannover.
Archenhold, F. S., Astronom, Villenkolonie Grunewald bei Berlin.
Bacharach, J., Reallehrer an der Realschule, Erlangen.
Bauer, G., Professor an der Universität, München.
Bauschinger, J., Privatdocent an der Universität, München.
Beck, A., Professor am Polytechnicum, Riga.
10. Binder, W., Professor an der Fachschule für Maschinenwesen, Wiener-Neustadt.
Bjerknes, Professor an der Universität, Christiania.
Blaschke, E., Privatdocent an der Universität, Wien.
Bobek, K., Professor an der deutschen Universität, Prag.
Bock, A., Reallehrer an der Realschule, Rothenburg a. d. T.
Böger, R., Oberlehrer an der Realschule, Hamburg.
Bohlmann, G., Privatdocent an der Universität, Göttingen.
Boltzmann, L., Professor an der Universität, Wien.
Bolza, O., Professor an der University of Chicago, Chicago Ill.
Braunmühl, A. v., Professor an der technischen Hochschule, München.
20. Brill, A., Professor an der Universität, Tübingen.
Brückner, Oberlehrer am Real-Gymnasium, Zwickau.
Brunn, H., Privatdocent an der Universität, München.
Bruns, H., Professor an der Universität, Leipzig.
Buka, F., Professor am Realgymnasium, Charlottenburg, und an der technischen Hochschule, Berlin-Charlottenburg.
Burkhardt, H., Professor an der Universität, Göttingen.
Burmester, L., Professor an der technischen Hochschule, München.
Busche, E., Oberlehrer an der Hansaschule, Bergedorf bei Hamburg.

Cantor, G., Professor an der Universität, Halle.
Cantor, M., Professor an der Universität, Heidelberg.
30. Carajianides, A., früher Göttingen, jetzt Griechenland.
Czuber, E., Professor an der technischen Hochschule, Wien.
Dalwigk, v., Assistent an der technischen Hochschule, München.
Dantscher v. Kollesberg, V., Professor an der Universität, Graz.
Dedekind, R., Professor an der technischen Hochschule, Braunschweig.
Dickstein, S., Professor, Warschau.
Dingeldey, F., Professor an der technischen Hochschule, Darmstadt.
Döhlemann, K., Privatdocent an der Universität, München.
Doergens, R., Professor an der technischen Hochschule, Berlin-Charlottenburg.
Dyck, W., Professor an der technischen Hochschule, München.
40. Dziobek, O., Professor an der technischen Hochschule, Berlin-Charlottenburg.
Eberhard, V., Professor an der Universität, Halle a. S.
Emmerich, A., Oberlehrer am Gymnasium, Mülheim a. d. Ruhr.
Engel, F., Professor an der Universität, Leipzig.
Escherich, G. v., Professor an der Universität, Wien.
Färber, C., Oberlehrer an der Luisenstädtischen Oberrealschule, Berlin.
Fiedler, E., Professor an der Cantonschule, Zürich-Hottingen.
Finger, J., Professor an der technischen Hochschule, Wien.
Fink, K., Professor an der Realschule, Tübingen.
Finsterwalder, S., Professor an der technischen Hochschule, München.
50. Fischer, K., Assistent an der technischen Hochschule, München.
Franklin, F., Professor an der Johns Hopkins Universität, Baltimore.
Franz, J., Professor an der Universität, Königsberg i. Pr.
Fricke, R., Professor an der technischen Hochschule, Braunschweig.
Frobenius, G., Professor an der Universität, Berlin.
Fuchs, L., Professor an der Universität, Berlin.
Fuhrmann, A., Professor an der technischen Hochschule, Dresden.
Gegenbauer, L., Professor an der Universität, Wien.
Gerhardt, K. J., Gymnasial-Director a. D., Graudenz.
Götting, E., Oberlehrer am Gymnasium, Göttingen.
60. Godt, W., Oberlehrer am Katharineum, Lübeck.
Gordan, P., Professor an der Universität, Erlangen.
Graefe, F., Professor an der technischen Hochschule, Darmstadt.
Graf, Professor an der Universität, Bern.
Grassmann, H., Oberlehrer an der Latina, Halle a. S.
Greenhill, A. G., President London Math. Soc., Professor am Artillery College, London-Woolwich.
Grübler, M., Professor an der technischen Hochschule, Berlin-Charlottenburg.
Günther, S., Professor an der technischen Hochschule, München.
Gundelfinger, S., Professor an der technischen Hochschule, Darmstadt.
Gutzmer, A., Berlin.

70. Haas, K., Gymnasialprofessor, Wien.

Haentzschel, E., Oberlehrer an der dritten Realschule, Berlin, und Privatdocent an der technischen Hochschule, Berlin-Charlottenburg.

Hagen, J., Professor und Director der Sternwarte am Georgetown College, Washington. D. C.

Hamburger, M., Professor an der technischen Hochschule, Berlin-Charlottenburg.

Hartwig, E., Director der Sternwarte, Bamberg.

Hauck, G., Professor an der technischen Hochschule, Berlin-Charlottenburg.

Hecht, Professor am Melanchthon-Gymnasium, Nürnberg.

Heffter, L., Professor an der Universität, Giessen.

Helm, G., Professor an der technischen Hochschule, Dresden.

Helmert, F. R., Professor an der Universität, Berlin.

80. Henneberg, L., Professor an der technischen Hochschule, Darmstadt.

Henneke, Professor am Gymnasium, Preussisch-Friedland.

Henrici, O., Professor am City and Guilds of London Institute, London.

Hensel, K., Professor an der Universität, Berlin.

Hermes, J., Professor am Progymnasium, Königsberg i. Pr.

Hertzer, H., Professor an der technischen Hochschule, Berlin-Charlottenburg.

Herz, N., Astronom, Wien.

Hess, E., Professor an der Universität, Marburg.

Hettner, G., Professor an der technischen Hochschule, Berlin-Charlottenburg, und an der Universität, Berlin.

Heun, Oberlehrer an der ersten Realschule, Berlin.

90. Hilbert, D., Professor an der Universität, Königsberg i. Pr.

Hölder, O., Professor an der Universität, Tübingen.

Holländer, E., Marine-Oberlehrer auf S. M. Schiff „Stosch“.

Hoppe, R., Professor an der Universität, Berlin.

Horn, J., Privatdocent an der technischen Hochschule, Berlin-Charlottenburg.

Hossfeld, C., Oberlehrer am Gymnasium, Eisenach.

Hurwitz, A., Professor am Polytechnicum, Zürich.

Hurwitz, J., Halle a. S.

Jahnke, E., Oberlehrer an der achten Realschule, Berlin.

Järisch, P., Oberlehrer am Johanneum, Hamburg.

100. Joukovsky, N., Professor an der Universität, Moskau.

Jürgens, E., Professor an der technischen Hochschule, Aachen.

Junker, F., Professorats-Candidat, Urach (Württemberg).

Kasten, H., Oberlehrer am Gymnasium, Bremen.

Keck, L., Professor am Realgymnasium, Nürnberg.

Kepinski, S., Universität, Krakau.

Kerschensteiner, G., Stadtschulrath, München.

Kiepert, L., Professor an der technischen Hochschule, Hannover.

Killing, W., Professor an der Akademie, Münster i. W.

Kleiber, J., Hauptlehrer an der Handelsschule, München.

110. Klein, F., Professor an der Universität, Göttingen.
Klein, G., Rector des Realgymnasiums, München.
Kneser, A., Professor an der Universität, Dorpat.
Knoblauch, J., Professor an der Universität, Berlin.
Köhler, C., Professor an der Universität, Heidelberg.
König, J., Professor an der technischen Hochschule, Budapest.
Königsberger, L., Professor an der Universität, Heidelberg.
Köpke, A., o. Lehrer an der Realschule, Ottensen.
Kötter, E., Professor an der Universität, Berlin.
Kötter, F., Professor an der Berg-Akademie, Berlin.
120. Kohn, G., Professor an der Universität, Wien.
Kostka, C., Professor am Gymnasium, Insterburg.
Kraft, F., Privatdocent am eidgen. Polytechnicum, Zürich.
Krause, M., Professor an der technischen Hochschule, Dresden.
Krazer, A., Professor an der Universität, Strassburg i. E.
Kühne, H., Erkner bei Berlin.
Kürschak, J., Privatdocent an der technischen Hochschule, Budapest.
Kullrich, Oberlehrer des Kadettenkorps, Gross-Lichterfelde.
Kutta, M., Assistent an der technischen Hochschule, München.
Lampe, E., Professor an der technischen Hochschule, Berlin-Charlottenburg.
130. Landsberg, G., Privatdocent an der Universität, Heidelberg.
Lerch, M., Docent am Böhm. Polytechnicum, Prag.
Lie, S., Professor an der Universität, Leipzig.
Lindemann, F., Professor an der Universität, München.
Lipschitz, R., Professor an der Universität, Bonn.
Lommel, E. v., Professor an der Universität, München.
London, F., Privatdocent an der Universität, Breslau.
Lüroth, J., Professor an der Universität, Freiburg i. B.
Mandl, M., Lehrer an der Realschule, Prossnitz in Mähren.
Mangoldt, H. v., Professor an der technischen Hochschule, Aachen.
140. Maurer, L., Professor an der Universität, Strassburg.
Mayer, A., Professor an der Universität, Leipzig.
Mehmke, R., Professor an der technischen Hochschule, Stuttgart.
Meyer, A., Professor an der Universität, Zürich.
Meyer, F., Professor an der Berg-Akademie, Clausthal.
Meyer, G., Lehrer an der Realschule, Bremen.
Meyer, G. F., Professor am Realgymnasium, München.
Meyer, Th., Oberlehrer am Gymnasium, Saarbrücken.
Minkowski, H., Professor an der Universität, Königsberg i. Pr.
Müller, F., Professor am Luisen-Gymnasium, Berlin.
150. Müller, Reinh., Professor an der technischen Hochschule, Braunschweig.
Müller, Rich., Oberlehrer an der Königl. Realschule, Berlin, und Privatdocent an der technischen Hochschule, Berlin-Charlottenburg.
Neuberg, J., Professor an der Universität, Lüttich.
Neumann, C., Professor an der Universität, Leipzig.

Netto, E., Professor an der Universität, Giessen.
Nöther, M., Professor an der Universität, Erlangen.
Papperitz, E., Professor an der Berg-Akademie, Freiberg i. S.
Pasch, M., Professor an der Universität, Giessen.
Pelz, C., Professor an der technischen Hochschule, Graz.
Peschka, A. V., Professor an der technischen Hochschule, Wien.
160. Pick, G., Professor an der Universität, Prag.
Piltz, A., Privatdocent an der Universität, Jena.
Pochhammer, L., Professor an der Universität, Kiel.
Pockels, F., Privatdocent an der Universität, Göttingen.
Pokrowsky, P., Professor an der Universität, Kiew.
Pringsheim, A., Professor an der Universität, München.
Prym, F., Professor an der Universität, Würzburg.
Rados, G., Professor an der technischen Hochschule, Budapest.
Recknagel, G., Rector des Realgymnasiums, Augsburg.
Reich, K., Diplom. Chemiker, Wien.
170. Reinhardt, C., Oberlehrer an der Fürstenschule, Meissen.
Réthy, M., Professor an der technischen Hochschule, Budapest.
Reuschle, C., Professor an der technischen Hochschule, Stuttgart.
Reye, Th., Professor an der Universität, Strassburg i. E.
Richarz, F., Professor an der Universität, Greifswald.
Richter, Oberlehrer am Gymnasium, Quedlinburg.
Riecke, E., Professor an der Universität, Göttingen.
Ritter, A., Professor an der technischen Hochschule, Aachen.
Rodenberg, C., Professor an der technischen Hochschule, Hannover.
Rogel, F., Ingenieur, Barmen.
180. Rohn, K., Professor an der technischen Hochschule, Dresden.
Rosanes, J., Professor an der Universität, Breslau.
Rosenow, H., Director der neunten Realschule, Berlin.
Rudel, K., Rector, Kempten.
Rudio, F., Professor am Polytechnicum, Zürich.
Runge, C., Professor an der technischen Hochschule, Hannover.
Saalschütz, L., Professor an der Universität, Königsberg i. Pr.
Schapira, H., Professor an der Universität, Heidelberg.
Scheffers, G., Privatdocent an der Universität, Leipzig.
Scheibner, W., Professor an der Universität, Leipzig.
190. Schell, W., Professor an der technischen Hochschule, Karlsruhe.
Schendel, L., Berlin.
Schering, E., Professor an der Universität, Göttingen.
Schilling, C., Professor an der Navigationsschule, Bremen.
Schilling, F., Assistent an der technischen Hochschule, Aachen.
Schlegel, V., Professor an der Gewerbeschule, Hagen i. W.
Schleiermacher, L., Professor an der Forstschule, Aschaffenburg.
Schlesinger, L., Professor an der Universität, Berlin.
Schlömilch, O., Geheimrat, Dresden.
Schmidt, Fr., Baumeister, Budapest.

200. Schmidt, M., Professor an der technischen Hochschule, München.
Schönflies, A., Professor an der Universität, Göttingen.
Scholz, P. G., Professor am Friedrichs-Realgymnasium, Berlin.
Schottky, F., Professor an der Universität, Marburg.
Schröder, E., Professor an der technischen Hochschule, Karlsruhe.
Schröder, Th., Professor am Melanchthon-Gymnasium, Nürnberg.
Schütz, J. R., Göttingen.
Schubert, H., Professor am Johanneum, Hamburg.
Schultz, E., Lehrer am Realgymnasium, Stettin.
Schumacher, H., Reallehrer an der Realschule, Neustadt a. H.
210. Schumacher, R., Reallehrer an der Realschule, Augsburg.
Schur, F., Professor an der technischen Hochschule, Aachen.
Schur, W., Professor an der Universität, Göttingen.
Schwarz, H. A., Professor an der Universität, Berlin.
Schwering, K., Director des Gymnasiums, Düren.
Seelhoff, P., Professor an der Navigationsschule, Bremen.
Seeliger, H., Professor an der Universität, München.
Seidel, Ph. L. von, Professor an der Universität, München.
Servus, H., Oberlehrer am Friedrichs-Realgymnasium, Berlin, und Privatdocent an der technischen Hochschule, Berlin-Charlottenburg.
Sidler, G., Professor an der Universität, Bern.
220. Siebert, A., Oberlehrer an der Hauptcadetten-Anstalt, Gross-Lichterfelde.
Sievert, H., Professor am Gymnasium, Bayreuth.
Simon, M., Professor am Lyceum, Strassburg i. E.
Sinram, H. Th., Hamburg.
Sommerfeld, A., Privatdocent an der Universität, Göttingen.
Souslow, Professor an der Universität, Kiew.
Sprung, A., Professor am Meteorologischen Institut, Berlin.
Stäckel, P., Professor an der Universität, Königsberg i. Pr.
Stahl, H., Professor an der Universität, Tübingen.
Staude, O., Professor an der Universität, Rostock.
230. Sterneck, R. v., Privatdocent an der Universität, Wien.
Stickelberger, L., Professor an der Universität, Freiburg i. B.
Stolz, O., Professor an der Universität, Innsbruck.
Study, E., Professor an der Universität, Bonn.
Sturm, R., Professor an der Universität, Breslau.
Tauber, A., Privatdocent an der Universität, Wien.
Thomae, J., Professor an der Universität, Jena.
Tötössy, B. v., Professor an der technischen Hochschule, Budapest.
Universitäts-Bibliothek zu Utrecht.
Valentin, G., Oberbibliothekar an der Königl. Bibliothek, Berlin.
240. Van Vleck, E. B., z. Z. Assistent am Polytechnicum, Zürich.
Veronese, G., Professor an der Universität, Padua.
Vogel, P., Professor an der Artillerie- und Ingenieurschule, München.
Voigt, W., Professor an der Universität, Göttingen.

Von der Mühll, K., Professor an der Universität, Basel.
Voss, A., Professor an der Universität, Würzburg.
Wälsch, E., Professor an der technischen Hochschule, Brünn.
Wallenberg, G., Oberlehrer an der neunten Realschule, Berlin.
Wangerin, A., Professor an der Universität, Halle.
Wassiljef, Professor an der Universität, Kasan.
250. Weber, E. v., Privatdocent an der Universität, München.
Weber, H., Professor an der Universität, Strassburg i. E.
Weierstrass, K., Professor an der Universität, Berlin.
Weiler, A., Privatdocent am Polytechnicum, Zürich.
Weingarten, J., Professor an der technischen Hochschule, Berlin-Charlottenburg.
Weinmeister, J. Ph., Professor an der Forst-Akademie, Tharand.
Weiss, W., Privatdocent an der technischen Hochschule, Prag.
Wellmann, H., Oberlehrer am Gymnasium, Bremen.
Weltzien, C., Professor an der Friedrichs-Werderschen Oberrealschule, Berlin.
Westermann, H., Oberlehrer an der Vorschule der technischen Hochschule, Riga.
260. Weyer, G. D., Professor an der Universität, Kiel.
Wiener, Chr., Professor an der technischen Hochschule, Karlsruhe.
Wiener, H., Professor an der technischen Hochschule, Darmstadt.
Wiltheiss, E., Professor an der Universität, Halle.
Wirtinger, W., Professor an der Universität, Innsbruck.
Witting, A., Oberlehrer am Gymnasium, Dresden-Strehlen.
Wölffing, E., Privatdocent an der technischen Hochschule, Stuttgart.
Wolf, M., Professor an der Universität, Heidelberg.
Zahradnik, K., Professor an der Universität, Agram.
Zindler, K., Privatdocent an der technischen Hochschule, Wien.
270. Ziwet, A., Professor an der University of Michigan, Ann Arbor, Mch.
Zorawski, C. v., Polytechnische Schule, Lemberg.
Zsigmondy, Privatdocent an der Universität, Wien.
Züge, Oberlehrer am Gymnasium, Lingen a. d. Ems.

Aus der Vereinigung ausgetreten:

Sievers, J., Oberlehrer, Frankenberg i. Sa.
Simon, H., Assistent an der Universitätsbibliothek, Berlin.

Adresse der Deutschen Mathematiker-Vereinigung zum achtzigsten Geburtstage des Herrn Karl Weierstrass. 31. October 1895.

Hochverehrter Herr Jubilar!

Sie blicken am heutigen Tage auf eine Lebensarbeit zurück, wie sie wenigen Sterblichen beschieden ist. Dankbar naht sich die wissenschaftliche Welt, um Ihnen ihre Glückwünsche darzubringen.

Die Vereinigung, zu der sich, dem Zuge unserer Zeit folgend, die Jünger der mathematischen Wissenschaft in unserem Vaterlande verbunden haben, und welcher sich eine grössere Zahl ausländischer Mathematiker angeschlossen hat, rechnet es sich zum Ruhme an, auch Sie, hochverehrter Herr Professor, zu den ihrigen zu zählen, und stolz auf diese Ehre darf sie sich an dem heutigen Feste betheiligen. Sind ja doch viele unter uns, die durch Ihre väterliche Hand in die Wissenschaft eingeführt wurden, und keiner, der nicht in Ihren Schriften eine unversiegbare Quelle reicher Belehrung und Anregung gefunden hat.

Es ist fast ein halbes Jahrhundert darüber hingegangen, seit Sie, den Spuren folgend, auf die Abel und Jacobi hingewiesen hatten, uns die Kenntniss der Abel'schen Functionen erschlossen. Sie haben damals schon, mit weiter schauendem Blick als die Zeitgenossen, jene functionentheoretischen Hilfsmittel geschaffen und mit Meisterschaft gehandhabt, die allein im Stande waren, in das neu erschlossene ausgedehnte Gebiet Licht zu bringen, mit denen nicht nur die ersten und einfachsten Fälle, sondern der ganze weite Bereich der neuen Transcendenten beherrscht werden konnte. So fundamental und weitreichend sind diese Methoden, dass sie in dem ganzen Gebiete der höheren Analysis neue Klarheit, scharfe und richtige Anschauungen geschaffen haben.

In immer erneuter Arbeit sind Sie zu ihnen zurückgekehrt, um ihnen

eine stets grössere Vollendung zu geben, um ihre Brauchbarkeit und Fruchtbarkeit an immer mehr Problemen zu beweisen.

Eine strenge Gewissenhaftigkeit in der Kritik der Beweise, eine das ästhetische Gefühl im höchsten Maasse befriedigende Ordnung und Schönheit in dem gegliederten Aufbau der Theorie, das sind die Grundzüge Ihrer Forschung, die uns als unerreichbares Muster dastehen. Sie durchdringt der philosophische Geist, der sich nicht mit der subjectiven Ueberzeugung von der Richtigkeit eines Resultates begnügt, der auch nach Klarheit strebt über die erkenntnisstheoretischen Gründe, auf denen diese Ueberzeugung ruht, nach Einsicht in die logische Berechtigung der angewandten Grundanschauungen, und mehr als einmal hat sich dabei gezeigt, dass weit verbreitete Ueberzeugungen und Anschauungen ungenau, unvollständig oder ganz unrichtig waren.

Wir dürfen Ihnen ein schönes Wort entgegenhalten, das wir im zweiten Bande Ihrer gesammelten Werke finden:

„Dass dem Forscher, so lange er sucht, jeder Weg gestattet ist, versteht sich von selbst. Es handelt sich um die systematische Begründung.“

Indem Sie geforscht und gesucht haben auf Wegen, die wir vielleicht nur zum kleinsten Theil kennen und übersehen, haben Sie reiche Schätze neuer Wahrheit aus der Tiefe zu Tage gefördert und im Geiste unseres grossen Gauss ein Gebäude aufgeführt, das durch die Klarheit der Anlage, die vollendete Schönheit der Durchbildung, die Strenge und Ordnung der Gedankenfolge dem wissenschaftlichen Sinn zur höchsten Befriedigung gereicht.

Wenn Sie die heutige Gestaltung der Mathematik überblicken, so müssen Sie mit gerechtem Stolze überall die Spuren Ihrer Wirksamkeit erkennen.

Immer sind Sie Ihren Schülern, die mit Dank zu Ihnen aufblicken, ein aufopfernder Führer und wahrer Freund gewesen, und wem es nur immer vergönnt war, mit Ihnen in persönliche wissenschaftliche Berührung zu kommen, der wird die Stunden dieses Verkehrs, denen er eine wesentliche Bereicherung seines wissenschaftlichen Besitzes verdankt, niemals vergessen.

Möge Ihnen ein gütiges Geschick einen langen und heiteren Lebensabend gewähren und Ihnen die Frische des Geistes, die wir heute bewundern, erhalten, der Wissenschaft zum Segen, Ihren Freunden und Verehrern zur Freude und Erhebung.

Der Vorstand der Deutschen Mathematiker-Vereinigung.

H. Weber, Vorsitzender.

A. Brill. G. v. Escherich. P. Gordan.

A. Wangerin. A. Gutzmer.

Zum Gedächtnis.

In die Gedächtnistafel der Deutschen Mathematiker-Vereinigung sind die Namen von fünf Mitgliedern einzutragen, deren Hinscheiden wir tief beklagen:

Wilhelm Ligowski, Professor an der Marineakademie zu Kiel, ist am 8. December 1893 im Alter von 72 Jahren einem Herzleiden erlegen. Der ihm gewidmete Nachruf stammt aus der Feder des Herrn Pochhammer.

Am 11. Juni 1894 ist Erhard Walder im 63. Lebensjahre an einem Gehirnschlage plötzlich verstorben. Im Jahre 1832 zu Nürnberg geboren, war er längere Zeit Lehrer der Gewerbeschule in Nördlingen, dann Rector der Gewerbeschule zu Kempten, von 1864—1879 Professor am Realgymnasium zu Regensburg und seitdem Professor am Realgymnasium in seiner Vaterstadt Nürnberg. Er hat Schulprogramme über Construction und Wirksamkeit der Blitzableiter und über theoretische Mechanik, sowie einen Grundriss der Arithmetik verfasst.

Julius Worpitzky, Professor am Friedrichs-Werderschen Gymnasium und an der Kriegsakademie zu Berlin, wurde am 4. März 1895 von langen, schweren Leiden erlöst. Der in den nachstehenden Blättern veröffentlichte Nekrolog nebst dem Schriftenverzeichnis Worpitzky's rührt von Herrn E. Lampe her.

Carl Prediger, Professor an der Bergakademie zu Clausthal, starb am 19. März 1895 im 73. Lebensjahre. Mit ihm ist, wie aus den von Herrn Fr. Meyer verfassten Zeilen hervorgeht, eine interessante Persönlichkeit von uns geschieden.

Ein tragisches Geschick hat endlich vor Kurzem eines der hoffnungsvollsten jüngeren Talente abgerufen. Ernst Ritter, bisher Privatdocent in Göttingen, ist am 22. September 1895 im Alter von 28 Jahren auf Ellis Island im Hafen von New-York vom Typhus dahingerafft worden, als er den neuen Continent betreten wollte, um einem ehrenvollen Rufe

an die Cornell University in Ithaca Folge zu leisten. Sein Andenken wird durch die sehr anerkennenden Worte geehrt, welche Herr F. Klein seiner Persönlichkeit und seinen wissenschaftlichen Leistungen und Bestrebungen im Folgenden gewidmet hat.

Des weiteren enthält die Chronik dieses Jahresberichtes ausführliche Nekrologe auf August Zillmer, Emil Weyr, Moriz Abraham Stern und Wilhelm Stahl, deren Ableben bereits im vorigen Berichte kurz erwähnt worden ist.

Schliesslich findet in diesem Jahresbericht ein aus der Feder des Herrn Wangerin stammender Nachruf für Franz Neumann Aufnahme, durch welchen die Deutsche Mathematiker-Vereinigung beabsichtigt, der allgemeinen Verehrung für diesen bedeutenden Forscher und Menschen ihrerseits Ausdruck zu geben.

August Zillmer.

Von einem Freunde.

Dr. phil. August Zillmer, Sohn eines Maurermeisters, am 23. Januar 1831 zu Treptow a. Rega geboren, besuchte zunächst die höhere Bürgerschule seiner Vaterstadt, auf der er im März 1847 die Abgangsprüfung ablegte. Mit dem Beginn des Sommersemesters 1847 trat er in die Untersecunda des Gymnasiums zum grauen Kloster in Berlin über, das er nach bestandenem Abiturientenexamen Ostern 1851 verliess, um auf der Berliner Universität Mathematik und Naturwissenschaften zu studiren. Nachdem er auf Grund einer nicht gedruckten Dissertation im Jahre 1858 von der Universität Rostock die Doctorwürde erhalten hatte, übernahm er in demselben Jahre die Stelle eines Mathematikers bei der Lebensversicherungs-Gesellschaft Germania in Stettin, aus der er im Jahre 1867 in die des zweiten Directors bei der neugegründeten Lebensversicherungs-Gesellschaft Nordstern in Berlin eintrat. Hier war er bis zum Jahre 1876 thätig, in welchem er in Folge der auf ihn gefallenen Wahl zum Director der Vaterländischen Lebensversicherungs-Gesellschaft nach Elberfeld übersiedelte.

Durch den Verlust des letzten Kindes, einer blühenden Tochter, war ihm der weitere Aufenthalt in Elberfeld verleidet, und um sich den Versicherungs-Wissenschaften ungestörter widmen zu können, gab er die Stellung im Jahre 1882 auf und lebte seit der Zeit in Berlin, wo er,

nachdem ihm auch seine Frau schon im Jahre 1883 im Tode vorausgegangen war, nach mehrmonatigen schweren asthmatischen Leiden am 22. Februar 1893 verstarb.

Unter seinem Namen sind von ihm veröffentlicht: 1) Die mathematischen Rechnungen bei Lebens- und Renten-Versicherungen. Berlin. Erste Aufl. 1861, zweite Aufl. 1887. 2) Beiträge zur Theorie der Prämien-Reserve. Stettin. 1863. Von ihm verfasst, aber anonym erschienen sind Sterbetafeln der deutschen Versicherungsanstalten.

Emil Weyr †.*)

Von

Gustav Kohn in Wien.

Emil Weyr wurde im Jahre 1848 in Prag als Sohn des Professors der Mathematik an der dortigen Staats-Oberrealschule Franz Weyr geboren. Im Hause Weyr hatten die mathematischen Wissenschaften eine Heimstätte. Von Jugend auf zum Mathematiker bestimmt, fand Emil in seinem Vater einen gediegenen Lehrer, in seinem jüngeren Bruder Eduard, der heute als Professor der Mathematik an der böhmischen technischen Hochschule in Prag wirkt, einen eifrigen Mitstrebenden.

Am Prager Polytechnicum, das er schon mit beträchtlichen Kenntnissen ausgestattet bezog, führte damals Wilhelm Fiedler seine Hörer in die neuere Geometrie ein und wusste die Prager wissenschaftlichen Kreise für diese Disciplin zu interessiren.

Emil Weyr fühlte sich durch ihre Reize mächtig angezogen und bald auch zu selbständiger wissenschaftlicher Thätigkeit angeregt. Eine bei Teubner in Leipzig erschienene Schrift, deren erster Theil (1869) eine constructive Theorie der rationalen Curven dritter Ordnung, deren zweiter Theil (1870) eine Theorie der Regelflächen dritter Ordnung, beides auf Grundlage der (1, 2)-Correspondenz zum Gegenstande hat, lenkte wohl zuerst die Aufmerksamkeit weiterer Kreise auf den jugendlichen Mathematiker.

Seine Vorliebe für die synthetische Geometrie wurde durch eine wissenschaftliche Reise nach Italien stark vertieft. Hatten die Arbeiten

*) Dieser Nachruf ist zuerst in den Monatsheften für Mathematik und Physik, Bd. VI erschienen (ohne das zugefügte Verzeichnis von Weyr's wissenschaftlichen Publicationen).

und der Ruf Cremona's den jungen Mathematiker nach Italien gezogen, so gelang es der persönlichen Einwirkung dieses Forschers, ihn ganz zu gewinnen. Der Einfluss Cremona's war ein nachhaltiger. Für seine ganze wissenschaftliche Laufbahn blieb Emil Weyr der synthetischen Geometrie und innerhalb derselben der Chasles-Cremona'schen Richtung treu, welche das Heranziehen von allgemeinen, nur analytisch begründeten Sätzen zu geometrischen Folgerungen nicht verschmäht. Die rein-geometrische Staudt-Reye'sche Richtung hat wenig Einfluss auf ihn gewonnen. Innerhalb jener Richtung suchte er sich aber selbständig seinen Weg.

Man kann recht wohl von einer ihm eigenthümlichen Methode sprechen, die in vielen gerade seiner hervorragendsten Arbeiten zu Tage tritt und sich folgendermaassen charakterisiren lässt. Aus einer bekannten Eigenschaft eines geometrischen Gebildes wird eine neue (ihr äquivalente) Eigenschaft einer gewissen algebraischen Correspondenz abgeleitet. Jene Eigenschaft erscheint dadurch gewissermaassen abstracter gefasst und von dem besonderen Gebilde losgelöst. Sie lässt sich jetzt in Eigenschaften der verschiedensten Gebilde umsetzen, an denen es gelingt, eine Correspondenz der betrachteten Art durch irgendwelche geometrische Constructionen hervorzurufen.

Die Methode lässt, wie man sieht, der Geschicklichkeit und der Erfindungsgabe des Geometers einen weiten Spielraum, und Weyr handhabte sie mit wahrer Meisterschaft.

So ist denn deutlich, wie durch ihn die Theorie der algebraischen Correspondenzen auf rationalen Trägern und Hand in Hand mit ihr die Theorie der rationalen Gebilde, insbesondere der rationalen Curven, gefördert wurde.

Die Theorie der algebraischen Correspondenzen, sowohl der allgemeinen, als auch insbesondere von speciellen unter ihnen, dankt ihm eine Reihe von einfachen Sätzen, und ein Theil der heute auf diesem Gebiete allgemein üblichen Terminologie rührt von ihm her. In Sonderheit der Theorie einer ganz besonders wichtigen Klasse von Correspondenzen hat er seine intensive Aufmerksamkeit zugewendet, nämlich der Theorie der Involutionen. Indem er neben den Involutionen erster Stufe, von denen er die kubischen besonders eingehend studirt hat, später, durch „Abbildung" rationaler Curven auf einander veranlasst, auch die Involutionen höherer Stufen untersuchte, hat er sich ein bleibendes Verdienst um die Wissenschaft erworben.

Handelt es sich um geometrische Untersuchung einer Correspondenz,

so wird in der Regel ein Kegelschnitt als ihr Träger angesehen und ihre „Directionscurve", die Einhüllende der Verbindungslinien entsprechender Punkte, studirt. Bekannte Eigenschaften von Correspondenzen werden vorwiegend dadurch verwertet, dass neben Kegelschnitten rationale Curven 3. und 4. Ordnung (sowohl ebene als Raumcurven) als Träger der Correspondenz angenommen werden. Wenn auf diese Art auch stellenweise Eigenschaften von nichtrationalen Gebilden als „Erzeugnissen" der Correspondenzen sich ergeben, so liegt doch nur eine Methode für das Studium von rationalen Gebilden vor, und diese stehen auch bei Weyr bis zum Jahre 1883 im Vordergrund des Interesses. Für das Studium einiger specieller rationaler Curven hat er bei rechnender Behandlung in mehreren Arbeiten auch noch die Parameterdarstellung herangezogen und erfolgreich verwertet.

Vom Jahre 1883 angefangen, gewinnen seine Arbeiten eine andere Richtung. Statt der Curven vom Geschlechte Null bilden von nun an die Curven vom Geschlechte Eins den Gegenstand seiner Forschungen. Den allgemeinen, bahnbrechenden Betrachtungen, durch welche Clebsch, Brill und Nöther mit so glänzendem Erfolge in die Geometrie auf einer algebraischen Curve eingedrungen waren, zögerte er sich anzuschliessen. Er hatte hier seine eigenen Anschauungen. Sein ganzes Streben war darauf gerichtet, auf diesem Gebiete mit seinen mehr elementaren Methoden vorzudringen. Als ihm (1883) der erste Schritt auf diesem Wege gelang, der ihm die Einsicht in die geometrische Natur der algebraischen eindeutigen Transformationen einer allgemeinen Curve dritter Ordnung in sich erschloss, erfüllte ihn dieser Erfolg, wie dem Schreiber dieser Zeilen in lebendiger Erinnerung ist, mit grosser Freude. Diese Einsicht ward denn auch die Basis für seine weiteren Untersuchungen über die Curven vom Geschlecht Eins, als deren schönste Früchte zahlreiche von ihm entdeckte elegante Eigenschaften der Raumcurven fünfter und sechster Ordnung vom Geschlecht Eins anzusehen sind.

Ein Blick auf das weiter unten abgedruckte Verzeichnis von Weyr's wissenschaftlichen Publicationen lässt seine erstaunliche Fruchtbarkeit erkennen. Er war ein rastloser, nimmer müder Arbeiter, als ob er geahnt hätte, dass der Zeit seiner Thätigkeit enge Grenzen gesteckt seien.

Das Bild der Wirksamkeit Emil Weyr's wäre ein ganz unzulängliches, wenn wir nicht auch seiner Lehrthätigkeit gedächten.

Seine Vorlesungen an der Wiener Universität waren schlicht und schmucklos, dabei aber von musterhafter Klarheit, so dass auch der Minderbegabte ihnen mühelos folgen konnte. Wenn unter den Mittel-

schullehrern Oesterreichs geometrische Kenntnisse und Verständnis für die Methoden der Geometrie weit verbreitet sind, so ist das vor allem sein Verdienst. Ihm ist vielfach auch zu danken, wenn während der Zeit seiner Wiener Wirksamkeit die wissenschaftliche mathematische Production in Oesterreich eine sehr erhebliche Steigerung erfahren hat, die in den betreffenden Jahrgängen der Sitzungsberichte der Wiener Akademie der Wissenschaften zum deutlichen Ausdruck kommt, wo die mathematischen Arbeiten einen breiten Raum einnehmen und überwiegend geometrische Untersuchungen zum Gegenstande haben. Der grösste Teil dieser Untersuchungen rührt von ihm und seinen Schülern her, unter denen nur der ihm im Tode vorausgegangene Ameseder hier mit Namen angeführt werden möge.

In Gemeinschaft mit Professor Gustav Ritter von Escherich hat er 1890 die Monatshefte für Mathematik und Physik begründet.

Glatt und klar war seine Laufbahn, ohne Kämpfe und Entbehrungen. In jungen Jahren stieg er die Stufenleiter der akademischen Carrière hinan. Im Jahre 1848 geboren, wurde er 1871 zum ausserordentlichen Professor am böhmischen Polytechnicum in Prag ernannt und 1875 als ordentlicher Professor an die Universität Wien berufen. An Auszeichnungen hat es ihm nicht gefehlt. Er war unter anderem wirkliches Mitglied der Akademie der Wissenschaften in Wien und der Franz-Josefs-Akademie in Prag, und kurz vor seinem Tode erhielt er die Ernennung zum Hofrath. Seit 1877 mit Marie Waniek von Domyslow in glücklichster Ehe, der zwei Söhne und eine Tochter entstammen, vermählt, wäre ihm kaum ein Wunsch übrig geblieben. Da sandte der Neid der Götter ihm eine tückische Krankheit, der er im besten Mannesalter nach langem Leiden erlag.

Emil Weyr's wissenschaftliche Publicationen.

Königl. Böhm. Gesellschaft der Wissensch.

Ueber die Doppelelemente projectivischer Gebilde und deren Bedeutung für Curven dritter Ordnung und Klasse. Sitzungsber. 1869. I. p. 3.

Ueber die Erweiterung der Giltigkeit der Entwicklung einer Quadratwurzel in einen Kettenbruch. Ibid. 1869. I. p. 18.

Ueber den perspectivischen Zusammenhang der Raumcurven dritter Ordnung mit den ebenen Curven dritter Ordnung vierter Klasse, und jener dritter Klasse vierter Ordnung. Ibid. 1869. I. p. 22.

Ueber die Curve der grössten und kleinsten elektromagnetischen Wirkung. Ibid. 1869. I. p. 59.

Ueber Kegelschnitte, welche einem Dreieck ein- oder umgeschrieben sind und einen festen Kegelschnitt doppelt berühren. Ibid. 1869. II. p. 5.

Ueber algebraische Curven. Ibid. 1869. II. p. 33.
Ueber höhere Involutionen. Ibid. 1870. I. p. 14.
Zur Geometrie der Curven dritter Ordnung. Ibid. 1870. I. p. 43.
Ueber die Krümmung windschiefer Flächen. Ibid. 1870. II. p. 29.
Die Erzeugung algebraischer Curven durch mehrdeutige Elementargebilde. 1870. Abh. VI. Folge, 4. Bd.
Ueber die Fusspunktcurven räumlicher Curven. Sitzungsber. 1871. I. p. 3.
Ueber die Fernwirkung elektrischer Solenoide und materieller ebener Flächen. Ibid. 1871. I. p. 25.
Ueber die involutorischen Winkelrelationen der Cardioide. Ibid. 1871. II. 69.
Erzeugnisse mehrdeutiger Elementargebilde im Raume. (Als Fortsetzung des Aufsatzes: „Die Erzeugung algebraischer Curven.“) 1871. Abh. VI. Folge, 5. Bd.
Ueber die Grundaufgabe der Involutionen dritten Grades. Sitzungsber. 1872. I. p. 28.
Ueber die Singularitäten der zweiten Ordnung bei rationalen ebenen Curven. Ibid. 1872. I. p. 59.
Ueber rationale Curven. Ibid. 1872. II. p. 9, 77, 81.
Ueber das Problem der Normalen bei Raumcurven. Ibid. 1873. p. 344.
Ueber Durchschnittspunkte von Focalen mit Kreisen und mit Lemniscaten. Ibid. 1873. p. 166.
Ueber Punktsysteme auf rationalen Curven. Ibid. 1873. p. 70.
Ueber die lineale Construction der Curven n-ter Ordnung mit einem $(n-1)$-fachen Punkte und der Curven n-ter Klasse mit einer $(n-1)$-fachen Tangente. Ibid. 1873. p. 198.
Die Lemniscate in rationaler Behandlung. 1873. Abh. VI. Folge, 6. Bd.
Ueber Curven vierter Ordnung. Sitzungsber. 1874. p. 164.
Grundzüge einer Theorie der cubischen Involutionen. 1874. Abh. VI. Folge, 7. Band.
Bemerkungen über eine besondere Art involutorisch liegender Kegelschnitte. Sitzungsber. 1876. p. 42.
Die Curven dritter Ordnung als Involutionscurven. Ibid. 1877. p. 131.
Ueber rationale Raumcurven. Ibid. 1882. p. 158.

Kais. Akademie der Wissenschaften in Wien.

Ein Versuch, das Newton'sche Gravitationsgesetz aus molecularen Kräften abzuleiten. Bd. LIV, I. Abth. p. 476 II. Abth. p. 630.
Ein Beitrag zur Theorie transversal-magnetischer Flächen. Bd. LVI, II. Abth. p. 666, 669—681. 1867.
Studien aus der höheren Geometrie. (Mit 1 Tafel.) Bd. LVII, II. Abth. p. 430, 449—466. 1868.
Ueber Krümmungslinien der Flächen zweiten Grades und confocale Systeme solcher Flächen. Bd. LVIII, II. Abth. p. 35, 60—83. 1868.
Zur Erzeugung der Curven dritter Ordnung. (Mit 1 Holzschnitt.) Bd. LVIII, II. Abth. p. 404, 633—644. 1868.
Die Dreitheilung eines Winkels. Bd. LVIII, I. Abth. p. 360. II. Abth. p. 655.

Construction des Krümmungskreises für Fusspunktcurven. (Mit 5 Holzschnitten.) Bd. LIX, II. Abth. p. 104, 169—176. 1869.

Ueber kaustische Brennlinien. Bd. LIX., I. Abth. 291, II. Abth. p. 469.

Ueber Curvenbüschel. Bd. LXI., II. Abth. p. 35, 82—88.

Zur Vervollständigung der Involutionen höherer Ordnung. (Mit 2 Holzschnitten.) Bd. LXI, II. Abth. p. 488, 600—606. 1870.

Geometrische Mittheilungen (I.). Bd. LXI, II. Abth. p. 651, 731—738.

Geometrische Mittheilungen (II.). Bd. LXI, II. Abth. p. 768, 819—827.

Geometrische Mittheilungen (III.). Bd. LXII, II. Abth. p. 147, II. Abth. p. 273.

Ueber Evoluten räumlicher Curven. Bd. LXII, II. Abth. p. 801, 804—808. 1870.

Ueber rationale Raumcurven vierter Ordnung. Bd. LXIII, II. Abth. p. 419, 493—504.

Ueber rationale ebene Curven vierter Ordnung, deren Doppelpunktstangenten Inflexionstangenten sind. Bd. LXVII, II. Abth. p. 286—287. 1873.

Die Erzeugung der Curven dritter Ordnung mittels symmetrischer Elementensysteme zweiten Grades. Bd. LXIX, II. Abth. p. 784—794.

Ueber Raumcurven vierter Ordnung mit einem Cuspidalpunkte. Bd. LXXI, II. Abth. p. 400—409. 1875.

Ueber die Abbildung einer rationalen Raumcurve vierter Ordnung auf einen Kegelschnitt. Bd. LXXII, II. Abth. p. 686—706. 1875.

Weitere Bemerkungen über die Abbildung einer rationalen Raumcurve vierter Ordnung auf einen Kegelschnitt. Bd. LXXIII, II. Abth. p. 203—220. 1876.

Ueber die projectivische Beziehung zwischen den singulären Elementen einer cubischen Involution. Bd. LXXIII, II. Abth. p. 654—656. 1876.

Ueber Raumcurven vierter Ordnung mit einem Doppelpunkte. Bd. LXXV. II. Abth. p. 168—174. 1877.

Ueber Punktsysteme auf rationalen Raumcurven vierter Ordnung. Bd. LXXV. II. Abth. p. 458—462. 1877.

Ueber die Abbildung einer mit einem Cuspidalpunkte versehenen Raumcurve vierter Ordnung auf einen Kegelschnitt. Bd. LXXVIII, II. Abth. p. 336—398. 1878.

Ueber die Abbildung einer Raumcurve vierter Ordnung mit einem Doppelpunkte auf einen Kegelschnitt. Bd. LXXVIII, II. Abth. p. 891—895. 1878.

Ueber die Abbildung einer rationalen ebenen Curve dritter Ordnung auf einen Kegelschnitt. Bd. LXXIX, II. Abth. p. 429—446. 1879.

Ueber Involutionen n-ten Grades und k-ter Stufe. Bd. LXXIX, II. Abth. p. 680—698. 1879.

Ueber dreifach berührende Kegelschnitte einer ebenen Curve dritter Ordnung und vierter Klasse. Bd. LXXX, II. Abth. p. 1040—1046. 1879.

Ueber vollständige eingeschriebene Vielseite. Bd. LXXXI, II. Abth. p. 80—84. 1880.

Bemerkung über Herrn C. Le Paige's Abhandlung: „Ueber eine Relation zwischen den singulären Elementen cubischer Involutionen. Bd. LXXXI, II. Abth. p. 162—164. 1880.

Ueber Projectivitäten und Involutionen auf ebenen rationalen Curven dritter Ordnung. Bd. LXXXI, II. Abth. p. 169—195. 1880.

Ueber Polargruppen. Bd. LXXXI, II. Abth p. 841—844. 1880.

Ueber biquadratische Involutionen zweiter Stufe und ihre typischen Curven. Bd. LXXXI, II. Abth. p. 1007—1031. 1880.

Notiz über harmonische Mittelpunkte eines Quadrupels. Bd. LXXXI, II. Abth. p. 1218—1219. 1880.

Ueber die involutorische Lage sich berührender Kegelschnitte. Bd. LXXXIII, II. Abth. p. 63—68. 1881.

Ueber biquadratische Involutionen erster Stufe. Bd. LXXXIII, II. Abth. p. 300—320. 1881.

Ueber Involutionen zweiter Stufe. Bd. LXXXIII, II. Abth. p. 349—350. 1881.

Ueber Ausartungen biquadratischer Involutionen und über die sieben Systeme der eine rationale Plancurve vierter Ordnung vierfach berührenden Kegelschnitte. Bd. LXXXIII, II. Abth. p. 807—828. 1881.

Notiz über Regelflächen mit rationalen Doppelcurven. Bd. LXXXIV, II. Abth. p. 691—692. 1881.

Ueber mehrstufige Curven- und Flächensysteme. Bd. LXXXIV, II. Abth. p. 884—907. 1881.

Ueber die Bedeutung des räumlichen Nullsystems für cubische Involutionen beider Stufen. Bd. LXXXIV, II. Abth. p. 1264—1290. 1881.

Ueber Flächen sechsten Grades mit einer dreifachen cubischen Curve. Bd. LXXXV, II. Abth. p. 513—525. 1882.

Ueber gemeinschaftliche Bisecanten algebraischer Raumcurven. Bd. LXXXV, II. Abth. p. 840—843. 1882.

Ueber einen Correspondenzsatz. Bd. LXXXVII, II. Abth. p. 592—594. 1883.

Ueber eindeutige Beziehungen auf einer allgemeinen ebenen Curve dritter Ordnung. Bd. LXXXVII, II. Abth. p. 837—872. 1883.

Ein Beitrag zur Gruppentheorie auf den Curven vom Geschlechte Eins. Bd. LXXXVIII, II. Abth. p. 436—482. 1883.

Ueber Raumcurven fünfter Ordnung vom Geschlechte Eins. (Erste Mittheilung.) Bd. XC, II. Abth. p. 206—225.

Ueber Raumcurven fünfter Ordnung vom Geschlechte Eins. (Zweite Mittheilung.) Bd. XCII, II. Abth. 1885.

Ueber Raumcurven fünfter Ordnung vom Geschlechte Eins. (Dritte Mittheilung.) Bd. XCVII, II. Abth. p. 592—617. 1889.

Ueber Raumcurven sechster Ordnung vom Geschlechte Eins. (Erste Mittheilung.) Bd. XCIX, II. Abth. p. 932—951. 1891.

Ueber Raumcurven sechster Ordnung vom Geschlechte Eins. (Zweite Mittheilung.) Bd. C, II. Abth. p. 457—466. 1891.

Ueber Involutionen höheren Grades auf nicht-rationalen Trägern. Bd. C., II. Abth. p. 589—606. 1891.

Ueber Vervollständigung von Involutionen auf Trägern vom Geschlechte Eins und über Steiner'sche Polygone. (Mit 1 Textfigur.) Bd. CI, II. Abth. p. 1457—1483. 1892.

Ueber abgeleitete I_n^{n-1} auf Trägern vom Geschlechte Eins. Bd. CI, II. Abth. p. 1506—1519. 1892.

Ueber Vervollständigung von Involutionen auf Trägern vom Geschlechte Eins und über Steiner'sche Polygone. (Zweite Mittheilung. Mit 3 Textfiguren.) Bd. CI, II. Abth. p. 1695—1741. 1892.

Journal für reine und angewandte Mathematik.

Ueber Involutionen höherer Grade. Bd. LXXII, S. 285—292.

Bestimmung der Anzahl involutorischer Elementenpaare einförmiger mehrdeutiger Gebilde. Bd. LXXIV, S. 189—192.

Ueber Normalen rationaler Raumcurven. Bd. LXXIV, S. 277—278.

Ueber die Anzahl der Doppelnormalen einer rationalen Raumcurve. Bd. LXXIV, S. 279—280.

Rendiconti del R. Istituto Lombardo.

Sopra una certa curva gobba di quart' ordine. Serie VII, vol. IV. 1871.

Intorno all' involuzione cubica nella quale hanno luogo proprietà anarmoniche. Vol. IV, fasc. VII. 1871.

Intorno alle cubiche gobbe. Vol. IV, fasc. XVII. 1871.

Sopra una proprietà metrica della cardioide. Vol. V, fasc. IV. 1872.

Sopra le proprietà involutorie d'un esagono gobbo e d'un esaedro completo. Serie II, vol. VI, fasc. V. 1873.

Sulle curve gobbe razionali. Serie II, vol. XV, fasc. VII. 1882.

Schlömilch, Zeitschrift.

Ueber magnetische Fernwirkung elektrischer Ströme und Stromringe. XIII. p. 413—440. 1867.

Ueber die Identität der Brennlinien mit den Evoluten der Fusspunktcurven. XIV. 1869.

Zur Geometrie der Curven dritter Ordnung. XV. 1870.

Krümmungsverhältnisse eines Curvenbüschels in einem Scheitel. XV. 1870.

Ueber Punktsysteme auf Curven dritter Ordnung. XV. 1870.

Ueber algebraische Curven, deren Punkte sich mit einer Variablen in eindeutige Beziehung setzen lassen. XVI. 1871.

Zur Theorie der Involutionen höherer Grade. XVI. 1871.

Ueber rationale Raumcurven. XVI. 1871.

Ueber Normalen an Curven zweiter Ordnung. XVI. 1871.

Mathematische Annalen.

Erzeugung algebraischer Curven durch projectivische Involutionen. Bd. III, S. 34—44. 1871.

Construction der Hauptkrümmungshalbmesser und der Hauptkrümmungsrichtungen bei beliebigen Flächen. Bd. III, S. 228—235.

Ueber die Curven dritter Ordnung mit einem Doppelpunkte. Bd. III. S. 235—237.

Ueber rationale Curven vierter Ordnung. Bd. IV, S. 243—244. 1871.

Mémoires de la Société royale des sciences de Liège.

Sur les involutions supérieures, représentées sur un même support. Série II, t. X.

Annali di Matematica pura ed applicata.

Sopra la corrispondenza del seconde grado fra due sistemi semplicemente infiniti. 1871. Serie II, t. IV. Dal luglio 1870 al settembre 1871. p. 272.

Nota sopra alcune singolarità di second' ordine delle curve gobbe razionali. Ibid. p. 328.

Giornale di Matematiche.

Sulle curve piane razionali del terz' ordine, p. 145 vol. IX. 1871.

Intorno alle curve gobbe razionali, p. 217. Ibid.

Alcuni teoremi intorno alla „Focale à Noeud", p. 259. Ibid.

Intorno alle involuzioni di grado qualunque, p. 165 vol. X. 1872.

Quistioni, Francesco Siacci et Emilio Weyr, p. 188. Ibid.

Monatshefte, Wien.

Ueber die Anzahl der n-fachen Elemente einer I_{n-1}^{n} auf einem Träger vom Geschlechte Eins. II. 458.

Ueber Fünfecke, welche einer C_3 gleichzeitig ein- und umgeschrieben sind. IV. p. 120.

Ueber Vierecke, welche einer C_3 gleichzeitig ein- und umgeschrieben sind. Ibid. p. 154.

Archiv mathematiky a fysiky,

kteryz vydava Jednota ceskych mathematiku v Praze a rediguje staly tajemnik Dr. Emil Weyr.

Principes d'une théorie des systèmes symétriques d'éléments. Svazek I. 1876.

Sopra la curvatura delle linee gobbe di terz' ordine. Svazek I, p. 52. 1876.

Ueber Krümmungslinien. (Zur Wahrung der Priorität.) Svazek I, p. 78. 1876.

Académie royale de Belgique.

Sur les surfaces d'involution (3me série, tome III, nº 5; mai 1882).

Mémoires de la Société des sciences physiques et naturelles de Bordeaux.

Principes d'une théorie des systèmes symétriques d'éléments. 1874.

Comptes Rendus.

Sur les lignes de courbure des surfaces réglées, t. 78. 1874.

Bulletin de la Société Mathématique de France.

Quelques théorèmes nouveaux sur la lemniscate. t. I. 1875.

Zpravy Jednoty ceskych mathematiku.

Z novejsi geometrie: O involuci. II. V Praze. 1870.

Z novejsi geometrie: O promitavych vlastnostech kruhu, str. 5—18. 1871.

Drobnosti, str. 85—86. Ibid.

Casopis pro pestovani mathematiky a fysiky.

1. O trojuhelnicich kruhovych. Roc. I. str. 24.
2. Dve poucky o kuzeloseckach. I. 101.

3. Urcovani nekonecne vzdalenych prvku utvaru geometrickych. I. 161.
4. O kuzeloseckach a jich kruzich zakrivenosti. (Prednaska, kterouz prof. Emil Weyr dne 20. rijna 1872 zapocal novou cinnost Jednoty ceskych mathematiku.) II. 65.
5. Urcovani nekonecne vzdalenych prvku prostorovych utvaru geometrickych. II. 105.
6. O kruhu deviti bodu. II. 190.
7. O evolutach krivek rovinnych. II. 277.
8. O rovinnych racionalnich krivkach tretiho stupne. III. 24, 113, 193.
9. O involucich na krivkach tretiho stupne. IX. 145.
10. O rekurrentnim vzorci k sestrojovani rovnic involucnich. IX. 279.
11. O prometnosti cyklicke. XI. 191—265.

Selbständig erschienene Schriften.

Theorie der mehrdeutigen geometrischen Elementargebilde und der algebraischen Curven und Flächen als deren Erzeugnisse. Mit 5 Figurentafeln. Leipzig 1869. Teubner. gr. 8°.

Geometrie der räumlichen Erzeugnisse ein- und zweideutiger Gebilde, insbesondere Regelflächen dritter Ordnung. Leipzig 1870. Teubner. gr. 8°.

Beiträge zur Curvenlehre. Wien 1880. Hölder.

Die Elemente der projectivischen Geometrie. Erstes Heft. Theorie der projectivischen Grundgebilde erster Stufe und der quadratischen Involutionen. Mit 58 Holzschnitten. Wien 1883. Braumüller.

Zweites Heft. Theorie der Curven zweiter Ordnung und zweiter Klasse. Mit 19 Holzschnitten. Wien 1887. Braumüller.

Ueber die Geometrie der alten Aegypter. Vortrag, gehalten in der feierlichen Sitzung der kais. Akademie der Wissenschaften am 29. Mai 1884. Wien 1884. In Commission bei Gerolds Sohn.

Cremonovy geometrické transformace utvaru rovinnych. V Praze 1872. Ziva, Sbornik vedecky musea kralovstvi Ceskeho. X. V komisi Rivnace.

Zakladove vyssi geometrie. (Sepsali Dr. Emil Weyr a Eduard Weyr.)

Dil I. Theorie promitavych utvaru prvoradych. 1871.

Dil. II. Theorie krivek stupne druheho. 1874.

Dil. III. O primocarych plochach druheho stupne a o vztahu kollinearnem a reciprokem zakladnich utvaru druhoradych a tretiradych. 1878. Ziva, Sbornik vedecky musea kralovstvi Ceskeho. Odbor prirodovedecky a mathematicky. V Praze v komisi Fr. Rivnace. VIII, XI, XII.

Uvod do geometricke theorie krivek rovinnych sepsal Dr. Ludvik Cremona. Ceske, spisovatelem rozmnozene a opravene vydani, jez usporadal Emil Weyr. V Praze 1873. Majetkem a nakladem Jednoty ceskych mathematiku.

Erinnerung an Moriz Abraham Stern.

Nach **Ferdinand Rudio.***)

Geboren am 29. Juni 1807, verlebte Moriz Abraham Stern die Jugendjahre in seiner schönen, an historischen Erinnerungen und Anregungen so reichen Vaterstadt Frankfurt a. M. Ohne je die Schule besucht zu haben, ohne auch je durch ein Maturitätsexamen hindurchgegangen zu sein, erwarb er sich lediglich durch Privatunterricht die zum Universitätsbesuche erforderlichen Kenntnisse. Im Herbste 1826 bezog er die Universität Heidelberg, aber nicht, um vorerst Mathematik zu studiren, sondern um sich, dem Wunsche seiner frommen Mutter folgend, durch philologische Studien auf den Beruf eines Rabbiners vorzubereiten. Wenn ihn auch bald eine innere Neigung mit unwiderstehlicher Gewalt der mathematischen Wissenschaft zuführte, so blieb er doch den historisch-philologischen Studien bis an sein Lebensende treu und kehrte immer und immer wieder zu denselben zurück, namentlich dann, wenn er, durch Schicksalsschläge schwer getroffen, in veränderter wissenschaftlicher Beschäftigung neuen Lebensmut zu schöpfen suchte. Wir verdanken dieser seiner Neigung eine Reihe wertvoller Arbeiten. Ich nenne nur unter vielen anderen den in seiner gediegenen Gedrängtheit geradezu klassischen Aufsatz über Regiomontanus, den grossen Mathematiker der deutschen Renaissance, ferner das mit seinem Freunde Theodor Benfey gemeinschaftlich herausgegebene Werk über die Monatsnamen einiger alter Völker und den im Jahre 1850 unternommenen Versuch einer Lösung der Keilschrift. Ja, noch als 84jähriger Greis begann er, den vielen von ihm beherrschten Sprachen auch die russische hinzuzufügen, die er bald in dem Grade sich anzueignen wusste, dass er nicht nur mathematische Arbeiten, sondern auch Werke der russischen Nationallitteratur im Originale lesen konnte.

Doch kehren wir zu seiner Studienzeit zurück! Von seinem Freunde Dr. Reiss, einem Frankfurter Mathematiker, auf Gauss hingewiesen, widmete sich Stern in Göttingen unter dem „princeps mathematicorum“ mit solcher Begeisterung seiner Lieblingswissenschaft, dass er bereits 1829

---

*) Der nachstehende Nekrolog ist eine gekürzte Wiedergabe der Rede, welche Herr Rudio am Grabe Stern's den 2. Februar 1894 auf dem Friedhofe Rehalp bei Zürich gehalten und nebst einem Bildnisse Stern's und dem vollständigen Verzeichnisse der Schriften desselben in der Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich veröffentlicht hat.

der Facultät seine Doctordissertation vorlegen konnte. Mit dieser, die Theorie der Kettenbrüche behandelnden Arbeit betrat er zugleich ein Wissensgebiet, dem er den bei weitem grössten Teil seines Lebens gewidmet hat, das Gebiet der Zahlentheorie. Ein eigentümlicher Zufall wollte es, dass seine Doctorprüfung zugleich die erste von Gauss abgehaltene war, der später oft noch scherzend geäussert hat, er habe vor diesem Examen grössere Furcht gehabt, als sein Examinand.

Noch in demselben Jahre 1829 habilitirte sich Stern an der Göttinger Universität, der er nun als einer ihrer beliebtesten Lehrer mehr als ein halbes Jahrhundert in ununterbrochener Thätigkeit angehörte. An der gewaltigen Reform des mathematischen Universitätsunterrichtes, die sich in diesem Zeitraume vollzog, hat er einen bedeutenden Anteil gehabt. Hunderte von Schülern, die stets mit inniger Verehrung seiner gedachten, hat er in die mathematische Wissenschaft eingeführt, unter diesen solche, die, um nur Bernhard Riemann zu nennen, den grössten Mathematikern ihres Jahrhunderts sich beigesellten. Das Jahr 1848 brachte Stern, nach 19jährigem Privatdocententume, die Ernennung zum Extraordinarius, obwohl er sich schon seit lange durch ausgezeichnete Arbeiten einen geachteten Namen in der Wissenschaft erworben hatte. Erhielt er doch beispielsweise in dem Jahre 1841 gleichzeitig den Preis von der Brüsseler Akademie für eine Abhandlung über die quadratischen Reste und von der dänischen Akademie für eine Arbeit über die Auflösung der transcendenten Gleichungen! Als im Jahre 1859 Dirichlet starb und Riemann zu seinem Nachfolger ernannt wurde, konnte die Regierung endlich nicht mehr umhin, auch Stern ein Ordinariat zu verleihen.

Noch ein Vierteljahrhundert, nach schon 30jähriger akademischer Thätigkeit, wirkte Stern als Ordinarius in Göttingen. Da veranlasste ihn, im Herbste des Jahres 1884, der Verlust seiner einzigen Tochter, die Lehrthätigkeit aufzugeben und zu seinem Sohne nach Bern überzusiedeln. Als dieser dann im Jahre 1887 an das eidgenössische Polytechnicum berufen wurde, hatten wir die grosse Freude, mit dem neuen Collegen zugleich auch den ehrwürdigen Nestor der deutschen Mathematiker in Zürich begrüssen zu können. Die naturforschende Gesellschaft entbot ihm sofort als Willkomm die Ernennung zum Ehrenmitgliede und beglückwünschte ihn zwei Jahre später durch eine besondere Deputation zum 60jährigen Doctorjubiläum. Wiederum ein Jahr später, im Jahre 1890, feierten wir mit ihm ein Jubiläum ganz seltener Art: Stern's erster Beitrag zu dem Crelle'schen Journale war in dem

sechsten Bande desselben erschienen. Und 100 Bände später schloss er im 106. Bande die stattliche Reihe der diesem berühmten Journale zugewendeten wertvollen Beiträge ab.

Mit Moriz Stern sinkt der letzte Zeuge jener grossen Göttinger Zeit ins Grab, die durch die Namen Gauss, Wilhelm Weber, Dirichlet, Riemann, Clebsch bezeichnet ist. Mit allen diesen Männern und so vielen anderen seiner Fachgenossen, namentlich mit Eisenstein, war er in inniger Freundschaft verbunden. Aber auch ausserhalb des Kreises der Mathematiker hat er mit manchem hervorragenden Zeitgenossen die herzlichsten Beziehungen unterhalten, so mit Jacob Henle, dem berühmten Anatomen, von dem er so oft und so gerne erzählte, mit Stilling, dem Chirurgen und Physiologen, mit Berthold Auerbach und anderen, mit denen er nun im Tode vereint ist.

Wilhelm Stahl.

Von

Th. Reye und **A. Brill.**

In voller Manneskraft wurde Wilhelm Stahl der mathematischen Wissenschaft durch plötzlichen Tod entrissen; er starb am 19. April 1894 in Berlin am Herzschlage, 47 Jahre alt. Sein schlichtes humanes Wesen, sein Humor, seine gutmütige Derbheit und sein feines Zartgefühl werden Allen unvergesslich bleiben, welche dem treuen, neidlosen, gemütvollen Manne persönlich nahe getreten sind.

W. Stahl wurde am 8. September 1846 in Fränkisch Krumbach im Odenwald als Sohn des dortigen Pfarrers geboren. Nach dem frühzeitigen Tode des Vaters erzog ihn in Darmstadt seine noch lebende Mutter, an der er mit inniger Liebe hing. Er studirte 1864—68 am Schweizerischen Polytechnicum in Zürich die Ingenieurwissenschaften, 1868—70 an den Universitäten Giessen und Berlin Mathematik, und promovirte 1870 in Heidelberg. An dem Kriege 1870—71 nahm er Teil vor Metz und an der Loire als Freiwilliger der Hessischen Division. Nach kurzer Wirksamkeit als Ingenieur wurde er Ostern 1872 an die Aachener technische Hochschule berufen auf den Lehrstuhl für synthetische und darstellende Geometrie und Graphostatik. Zwanzig Jahre später, 1892, vertauschte er diese Professur mit einer analytisch-geometrischen an der technischen Hochschule in Charlottenburg, welcher er bis zu seinem Tode angehörte.

Nach Beendigung seiner Universitätsstudien wandte er sich zunächst mathematisch-physikalischen und mechanischen Untersuchungen zu, in denen seine Vorliebe für die Geometrie schon deutlich hervortritt. In seinen ersten beiden Abhandlungen*) bestimmt er für einen homogenen, von Ebenen und Flächen zweiter Ordnung begrenzten Körper sogenannte Potentialflächen, d. h. ungeschlossene Flächen, die so mit Masse belegt werden können, dass ihr Potential überall ausserhalb des Körpers mit dessen Potential gleichwertig wird. In drei anderen Arbeiten**) giebt er eine geometrische Theorie der parabolischen und der hyperbolischen Träger nebst äusserst einfachen Constructionen und Berechnungen der Spannungen, die bei veränderlicher Belastung in den Trägerstäben auftreten; ferner bestimmt er für ein System fest verbundener Einzellasten, die sich über einen gestützten Balken hinbewegen, geometrisch die Aenderungen des Seilpolygons und des Biegungsmomentes.

Seit 1876 nahm die Geometrie, erst die synthetische, dann auch die analytische, seine ganze Forscherkraft in Anspruch. Insbesondere hat er über gewisse Strahlensysteme, die quadratischen Strahlencomplexe und die rationalen ebenen und räumlichen Curven eine Reihe grösserer Arbeiten veröffentlicht und dadurch unsere Kenntnis derselben vielfach erweitert. Diese geometrischen Abhandlungen sind sehr reichhaltig, aber nicht leicht, grösstenteils sogar recht schwer zu lesen; denn er stellt darin grosse Anforderungen an sich und seine Leser und erspart diesen selbst die Ausfüllung von Lücken in der Beweisführung nicht ganz. Acht von diesen Abhandlungen sind synthetisch***), nämlich sechs liniengeometrische und zwei (Bd. 99 und 101), welche Untersuchungen über höhere Raumcurven und Flächen enthalten. An die letzteren beiden schliessen Stahl's analytisch-geometrische Arbeiten über rationale Curven sich an.

Die von Kummer analytisch ermittelten Strahlensysteme zweiter Ordnung oder zweiter Klasse ohne Brennlinien waren schon vor Stahl synthetisch abgeleitet und untersucht worden. Aber mit Recht hält W. Stahl es für „zweckmässig, verschiedenartige Herleitungen derselben zu benutzen, um alle wichtigeren Eigenschaften dieser complicirten Raumgebilde zu übersehen“. Er giebt (Bd. 91, 92, 95 und 97) drei neue Constructionen und Erzeugungen solcher Systeme und vervollständigt

*) Journal für d. r. u. a. Math. Bd. 79 und die Inaug.-Dissertation (Darmst. 1870).

**) Zeitschr. d. Vereins deutscher Ingenieure Bd. XX, XXI (1875—76). Die nachfolgenden Bemerkungen darüber verdanken wir Herrn Henneberg.

***) Journal f. Math. Bd. 91, 92, 93, 94, 95, 97, 99, 101.

zugleich deren Theorie. Beispielsweise erzeugt er (Bd. 97) das Strahlensystem zweiter Klasse vierter Ordnung durch zwei ebene Punktfelder, zwischen denen eine quadratische geometrische Verwandtschaft besteht, und erhält mittelst der beiden Hauptdreiecke der Felder sofort 14 singuläre Ebenen und sechs singuläre Punkte des Systemes. Auf drei Arten kann dieses System, wie leicht sich ergiebt, durch Regelscharen zweiten Grades beschrieben werden, deren Leitscharen drei mit ihm gleichartige Strahlensysteme bilden. Die vier Systeme haben eine und dieselbe Brennfläche vierter Klasse achter Ordnung, welche ausserdem von den Strahlen eines Systemes vierter Klasse sechster Ordnung doppelt berührt wird. Das letztere besteht, wie Stahl nachweist, aus den Geraden von ∞^1 Hyperboloiden, welche acht der singulären Ebenen berühren.

Von grossem Interesse ist Stahl's Untersuchung eines Strahlensystemes Σ_1 zweiter Ordnung ohne Brennlinie, welches unendlich viele Regelscharen zweiten Grades enthält (Bd. 95). Die Leitstrahlen dieser Scharen bilden ein System Σ_2 von gleicher Art und mit derselben Brennfläche wie Σ_1. Die Hyperboloide, auf denen die Regelscharen liegen, haben zu dreien acht Punkte gemein, welche singuläre Punkte beider Systeme sind, weil jeder von ihnen auf mehr als zwei Strahlen von Σ_1 resp. Σ_2 liegt. Die Hyperboloide gehen deshalb alle durch die acht Punkte und liegen in einem Flächenbündel. Sehr geschickt leitet Stahl hieraus beide Arten von Strahlensystemen zweiter Ordnung sechster Klasse ab und durch Specialisirung aus diesen die Systeme fünfter, vierter, dritter und zweiter Klasse. Zugleich aber gelangt er zu allen übrigen Strahlensystemen, die mit jenen die Brennflächen gemein haben.

Uebrigens setzt jede seiner drei Herleitungen von Strahlensystemen gewisse (singuläre) Punkte oder Ebenen, die imaginär sein können, als reell voraus und beschränkt sich damit auf einen der möglichen Hauptfälle. Von fast allen übrigen rein geometrischen Arbeiten Stahl's gilt das Gleiche, insbesondere auch bezüglich der Beweisführung.

Den Strahlencomplexen zweiten Grades sind zwei seiner Abhandlungen gewidmet. In der einen (Bd. 93) bestimmt er mit Hülfe der sechs Klein'schen Fundamentalcomplexe, die als reell vorausgesetzt werden, die Kegel und Kegelschnitte aller quadratischen Complexe, die eine gegebene Singularitätenfläche haben, und geht auch auf Herrn Schur's Erzeugung der quadratischen Complexe und auf deren Polarentheorie näher ein. In der anderen (Bd. 94) beweist er u. a. analytisch, dass die quadratischen Complexe mit gegebener Singularitätenfläche die Geraden

des Raumes zu zehnen gruppiren; und zwar ist jede Gerade einer Gruppe die Polare der neun übrigen in Bezug auf einen der Complexe. Im Falle tetraedraler Complexe werden die Geraden analog zu vieren gruppirt. Mit einer früheren Abhandlung (Bd. 91) hängen diese beiden zusammen durch die Strahlensysteme zweiter Klasse dritter Ordnung, welche von den „Polaraxen" einer Ebene μ und den Polaren der Geraden von μ bezüglich eines quadratischen Complexes gebildet werden.

Seine Publicationen über Raumcurven und Flächen eröffnet W. Stahl mit einer bemerkenswerten Abhandlung (Bd. 99) über solche Raumcurven R_{β_1}, welche wie die rationalen vierter Ordnung auf je einer Fläche β_1 zweiter Ordnung liegen, und deren Schmiegungsebenen je eine Fläche β zweiter Ordnung berühren. Dieselbe Grundeigenschaft haben dann der Ort R_β der Berührungspunkte dieser Ebenen, die Doppelcurven R_{γ_1} und R_γ der Tangentenflächen von resp. R_{β_1} und R_β, sowie die Raumcurven R_{α_1} und R_α, denen die zweifachen Berührungsebenen von R_{β_1} und R_β sich anschmiegen; doch können diese Curven in mehrere die Grundeigenschaft besitzende zerfallen. Die drei Raumcurven R_{γ_1}, R_γ und R_β stehen in derselben Beziehung zu einander, wie R_{β_1}, R_β und R_α. Ueberhaupt leitet Stahl aus einer solchen Raumcurve vier Systeme von ∞^2 collinearen Raumcurven ab, welche alle die Grundeigenschaft haben.

Salmon hat wohl zuerst bemerkt, dass die Gleichung der Tangentenfläche einer rationalen Raumcurve R_4 vierter Ordnung in die Gleichung der desmischen Fläche vierter Klasse 12. Ordnung (der verallgemeinerten Krümmungscentrenfläche eines Ellipsoides oder Hyperboloides) übergeht, wenn darin die Punktcoordinaten durch ihre Quadrate ersetzt werden. Diesen merkwürdigen Zusammenhang der beiden Flächen legt W. Stahl in seiner reichhaltigsten synthetischen Abhandlung (Bd. 101) klar, indem er eine eingehende Theorie der Raumcurve R_4 und der zu ihr reciproken Curve 6. Ordnung vorausschickt. Er gelangt rein geometrisch zu einer Schar cubischer Raumcurven, die auf der Tangentenfläche von R_4 liegen und mit R_4 je einen Punkt nebst dessen Tangente und Schmiegungsebene gemein haben. Die Tangenten und Axen dieser cubischen „Osculanten"*) von R_4 liegen mit den Tangenten von R_4 in einem tetraedralen Complexe K, dessen Haupttetraeder von den vier stationären Schmiegungsebenen α, β, γ, δ der R_4 gebildet wird. Die Osculanten werden durch die Tangenten von R_4 projectiv auf einander bezogen, ihre homologen Tangenten liegen in je einer Schmiegungsebene von R_4; ihre Schmiegungs-

*) So nennt er sie mit Herrn Jolles in späteren analytischen Arbeiten.

ebenen aber umhüllen eine Steiner'sche Fläche F_4 vierter Ordnung dritter Klasse, von welcher R_4 eine Haupttangentencurve ist. Die Punkte von R_4 und ebenso die Punkte dieser Fläche F_4 sind paarweise harmonisch getrennt durch zwei beliebige Gegenkanten eines Tetraeders $L_1L_2L_3L_4$, welches die drei Doppelgeraden von F_4 zu Kanten und deren Schnittpunkt L_4 zum Eckpunkt hat, und dessen übrige Eckpunkte L_1, L_2, L_3 harmonisch von L_4 getrennt sind durch je zwei Gegenkanten des Haupttetraeders $\alpha\beta\gamma\delta$.

Das Tetraeder $\alpha\beta\gamma\delta$ nun ist ein Poltetraeder von ∞^3 Flächen zweiter Ordnung f_2, und unter diesen giebt es ∞^1 Flächen F_2, welche dem Punkte L_4 je eine Schmiegungsebene von R_4 als Polarebene zuweisen. Die Flächen F_2 berühren die Ebenen des Tetraeders $L_1L_2L_3L_4$ und vier andere Ebenen, die mit jenen und den Ebenen α, β, γ, δ eine sog. desmische Configuration bilden. Sie umhüllen eine desmische Fläche vierter Klasse 12. Ordnung, die Brennfläche von drei Strahlensystemen zweiter Klasse sechster Ordnung; zwei dieser Systeme bestehen aus den Regelscharen der Flächen F_2, das dritte aber aus Strahlen des tetraedralen Complexes K. Wird nun das Gebüsch jener ∞^3 Flächen f_2 projectiv auf den Ebenenraum bezogen, indem man jeder f_2 die Polarebene von L_4 bezüglich dieser Fläche entsprechen lässt, so entspricht, wie sofort einleuchtet, der abwickelbaren Tangentenfläche von R_4 die von den Flächen F_2 umhüllte desmische Fläche. Aus den Eigenschaften der Raumcurve R_4 und ihrer Tangentenfläche ergeben sich dann ohne weiteres die Eigenschaften der desmischen Fläche. — Von dieser letzten synthetischen Abhandlung W. Stahl's ist hiemit der Gang der Entwickelung in Kürze angedeutet und ein Teil ihrer reichen Ergebnisse hervorgehoben.

Schon bei Gelegenheit früherer Arbeiten mag Stahl die Bemerkung gemacht haben, dass gewisse Eigenschaften der rationalen Curven erst in algebraischer Fassung zum prägnanten Ausdruck gelangen. In verhältnismässig kurzer Frist hatte er sich mit den Methoden der neueren Algebra bekannt gemacht. In den nun noch zu besprechenden sieben Abhandlungen, die fast ausschliesslich die rationalen Curven betreffen, hat er sie mit steigendem Erfolge angewendet.

Gleich die erste: „Ueber rationale ebene Curven vierter Ordnung“ (Journ. f. Math., Bde 101, 104) verbindet in fruchtbarer Weise die analytische mit der synthetischen Behandlung. Stahl's Abhandlungen über rationale Curven gehen alle von einer gewissen „Fundamental-Involution“ aus, die sich auf jedem Gebilde dieser Art vorfindet, und die man am einfachsten als die geometrische Einkleidung eines Begriffes

aus der Theorie der simultanen Binärformen von gleicher Ordnung definirt. Da Stahl diese Involution in den Mittelpunkt seiner Theorie stellt, sie aber nirgends ausdrücklich erklärt, so mag dies in den Bezeichnungen jener ersten Arbeit zunächst kurz geschehen.

Sind die homogenen Coordinaten x_1, x_2, x_3 eines Punktes der ebenen rationalen Curve vierter Ordnung dargestellt durch die Binärformen $f_1(\lambda, \mu)$, $f_2(\lambda, \mu)$, $f_3(\lambda, \mu)$, ist also, wenn ρ ein Proportionalitätsfactor ist,

$$(1) \quad \rho x_i = f_i(\lambda, \mu) = a_i \mu^4 + 4 b_i \mu^3 \lambda + 6 c_i \mu^2 \lambda^2 + 4 d_i \mu \lambda^3 + e_i \lambda^4, \quad (i = 1, 2, 3),$$

so nennt man eine andere biquadratische Form:

$$\varphi(\lambda, \mu) = A\lambda^4 + B\lambda^3\mu + C\lambda^2\mu^2 + D\lambda\mu^3 + E\mu^4$$

zu den drei Formen f „apolar“ oder „conjugirt“, wenn die drei Gleichungen bestehen:

$$A a_i - B b_i + C c_i - D d_i + E e_i = 0.$$

Durch diese ist φ nicht völlig bestimmt, vielmehr sind die Coefficienten A, B, ... lineare homogene Functionen der dreireihigen Determinanten [abc], [abd], ... mit noch einem willkürlichen Parameter τ. Man kann etwa setzen:

$$A = [dcb]; \quad B = [dca] + \tau[edc]; \quad C = [dba] + \tau[edb];$$
$$D = [cba] + \tau[ecb]; \quad E = \tau[dcb],$$

so dass also φ in der Form erscheint $\varphi = \varphi_1 + \tau\varphi_2$, wo φ_1 und φ_2 zwei bestimmte zu den f conjugirte Binärformen sind.

Betrachtet man nun die Gleichung:

$$(2) \qquad A\lambda^4 + B\lambda^3 + C\lambda^2 + D\lambda + E = 0,$$

so gehört zu jedem Werte von τ ein bestimmtes Quadrupel von Wurzeln λ_1, λ_2, λ_3, λ_4, das mit τ sich ändert, und das, als Parameterquadrupel der durch 1) dargestellten Curve (für $\mu = 1$) aufgefasst, auf dieser eine Punkt-Involution erster Stufe definirt.

Was die rationale ebene Curve nter Ordnung (C_n) angeht, so setzt sich die allgemeine zu den drei Formen nter Ordnung f_1, f_2, f_3 conjugirte Form φ linear aus $n-2$ speciellen solchen Formen $\varphi_1, \varphi_2, \ldots, \varphi_{n-2}$ zusammen; die Fundamental-Involution wird von der nten Ordnung und der $(n-3)$ten Stufe. — Analog giebt es für die rationale Raumcurve nter Ordnung vier Formen f, und $n-3$ hierzu conjugirte φ; die Involution ist von der $(n-4)$ten Stufe.

Für die ebene C_4 deutet Stahl diese Involution dadurch geome-

trisch, dass er an den früher erwähnten Begriff der „Osculanten" der Curve anknüpft, eines Systems von Curven, deren Coordinaten Formen proportional sind, die durch den Polarenprocess aus f_1, f_2, f_3 abgeleitet werden. Für die C_4 ist die zu einem Curvenpunkte λ_1 gehörige Osculante erster Ordnung eine rationale C_3. Besitzen die drei Wendepunkte dieser C_3 die Parameter λ_2, λ_3, λ_4, die dann dem λ_1 entsprechen, so zeigt es sich, dass dieses Entsprechen ein gegenseitiges ist; die Beziehung ist eben die jener Involution vierter Ordnung erster Stufe.

Die Coefficienten A, B, ... der Gleichung 2), also der conjugirten Form φ, verwendet nun Stahl zur Darstellung vieler mit der C_4 in Beziehung stehenden Gebilde. Die Coordinaten des „Wendekegelschnitts" sind quadratische Functionen derselben, in die Gleichung für die Parameter der Doppelpunkte gehen sie im dritten Grade ein u. s. w.

In dem zweiten Aufsatz über dieselbe Curve (Journ. f. Math. Bd. 104) ändert Stahl den Plan insofern ab, als er hier die Darstellung der zur Curve gehörigen invarianten Gebilde an eine (immer vorhandene) Binärform sechster Ordnung anschliesst, deren zweite partielle Differentialquotienten die den Coordinaten proportionalen Formen f_1, f_2, f_3 liefern. Die Wurzeln dieser Binärform, die ihrer Hessischen und anderer covarianten Formen, das Verschwinden gewisser Invarianten erfahren elegante Deutungen.

Auch für einige höhere rationale ebene und Raumcurven deutet Stahl (Journ. f. M. Bd. 104 S. 38) jene Fundamental-Involution durch geometrische Processe. Wieder sind es die ersten und zweiten Osculanten, deren stationäre Elemente die zu einem Curvenpunkt in Involution stehenden Parameterwerte geben. So wird der Raumcurve R_5 fünfter Ordnung durch die Involution eine solche R_3 zugeordnet, und diese Beziehung fördert neue Eigenschaften der R_5. Die Fruchtbarkeit jener Polaren-Operationen, die Stahl zu einem wichtigen Hülfsmittel der Untersuchung gestaltet hat, besteht darin, dass bekannte Eigenschaften von Curven niederer Ordnung, übertragen auf Curven-Systeme derselben Ordnung, die einer höheren Curve zugehören, für die Erforschung dieser höheren Anhaltspunkte gewähren. So bilden die Osculanten der R_6 ein System von R_5, deren zugeordnete R_3 eine Fläche zweiter Ordnung erzeugen. Eine solche entspricht nun wieder jeder ersten Osculante einer R_7 und dient, als Regelschar aufgefasst, dazu, die Involution auf dieser Curve auf die Punkte des Raumes abzubilden, u. s. w.

Den Begriff der „Apolarität" auch auf Raumcurven auszudehnen, und zwar durch involutorische Paarung von Curven gleicher Ordnung

und Klasse, unternimmt eine kleine Abhandlung im 107. Bande des J. f. M., auf die wir nicht näher eingehen.

In den beiden letzten grossen Abhandlungen Stahl's (Mathematische Annalen, Bde. 36, 40), aus denen auch eine Notiz über die Resultante (ebd. Bd. 35) hervorgegangen ist, handelt es sich darum, die einer rationalen Curve nter Ordnung ein-eindeutig zugeordneten „zu ihr perspectiven Strahlbüschel“ mter Ordnung ($m < n$), d. h. solche Curven mter Klasse darzustellen, deren Tangenten (Strahlen) durch die entsprechenden Punkte der C_n gehen, von denen also je zwei zu ihrer Erzeugung verwendbar sind; ferner um die Angabe von gleichfalls „perspectiven“ Curven niederer Ordnung, deren entsprechende Punkte nämlich je auf den Strahlen eines solchen Büschels liegen.

Stahl nimmt diese bekannte Fragestellung mit neuen Hülfsmitteln auf, die ihm eine Einteilung aller rationalen Curven nter Ordnung ermöglicht. Schon F. Meyer hatte sich die Aufgabe gestellt, von den erzeugenden Curven ausgehend, eine Klassification der rationalen C_4 vorzunehmen, und hatte eine erschöpfende Aufzählung aller Unterarten vorgenommen. Auch er legt dabei die conjugirten Formen φ_i zu Grunde. Aber Stahl verwendet weiter noch die Bemerkung, dass diese sich als Polarformen einer einzigen höheren Binärform auffassen lassen; hierdurch und durch eine eigentümliche Wendung des Eliminationsprocesses gelingt es ihm, die Gleichung der erzeugenden Gebilde nicht nur für die höheren ebenen, sondern auch für die räumlichen Curven aufzustellen und in ihrer Mannigfaltigkeit zu überschauen. Für die ebenen Curven C_n knüpft er, wie gesagt, statt an die den Coordinaten proportionalen Binärformen nter Ordnung, an die zu ihnen conjugirten $f_1, f_2, \ldots, f_{n-2}$ (vorher mit $\varphi_1, \varphi_2, \ldots$ bezeichnet) an, indem er die Coefficienten einer $(n-1)$ten Form f_{n-1}, die er beliebig zu den $n-2$ hinzunimmt, in geschickter Weise dazu verwendet, die Coordinaten eines unbestimmten Punktes, der in der Darstellung der covarianten Curven auftritt, einzuführen. So werden zunächst die Gleichungen der ∞^1 zu einer C_n perspectiven „Strahlbüschel $(n-1)$ter Ordnung“ (Klassencurven) in Gestalt einer verschwindenden Determinante mit einer Reihe willkürlicher Elemente dargestellt. Die Ordnung dieser Gleichung lässt sich nun erniedrigen, wenn man davon Gebrauch macht, dass sich die Formen $f_1, f_2, \ldots, f_{n-2}$ für $r \leqq \frac{1}{2}(n-3)$ immer als die rten Polaren einer Form $F^{n+r}(\lambda)$ von der $(n+r)$ten Ordnung darstellen lassen. Jeder ganzen Zahl r (zwischen -1 und $\frac{1}{2}(n-3)$) entsprechen auf diese Weise erzeugende Büschel, bis herab zur Ordnung $\frac{1}{2}n$ (bezw. $\frac{1}{2}(n+1)$ und $\frac{1}{2}(n-1)$)

— was übrigens schon bekannt war —, für irgend ein r giebt es noch ∞^{n-2r-3} Möglichkeiten, die Function F zu bestimmen.

Ferner existiren zu jedem Strahlbüschel, d. h. zu jeder Function $F^{n+r}(\lambda)$, noch Ordnungscurven $C_\omega(\omega = 0, 1, \ldots, \frac{1}{4}(n-3))$ in endlicher Anzahl t, die zu ihm perspectiv liegen und mit der gegebenen C_n $3\omega+2$ Punkte entsprechend gemeinsam haben. Ihre Existenz ergiebt sich daraus, dass man t Functionen $F(\lambda)$ finden kann, die sich durch eine Summe von $3\omega+2$ Potenzen linearer Functionen darstellen lassen.

In besonderen Fällen kann die Zahl r den Wert $\frac{1}{2}(n-3)$ übersteigen, womit sich die Ordnung der Büschel erniedrigt. Dies tritt für besondere Formen $f_1, f_2, \ldots, f_{n-2}$ ein, die dann einer Curve mit specielleren Eigenschaften entsprechen, was Stahl an Beispielen erläutert.

Diese schöne Abhandlung wird an Reichtum und Bedeutung der Ergebnisse noch übertroffen von Stahl's letzter Arbeit (Math. Ann. 40), welche die besprochene Untersuchungsmethode auf die rationalen Raumcurven und die zu ihnen perspectiven „Ebenenbüschel" (abwickelbaren Flächen) ausdehnt. Hier ist die Anzahl der zu den vier Coordinaten-Formen conjugirten f gleich $n-3$. Zunächst bieten sich wieder perspective Ebenenbüschel $(n-2)$ter Ordnung dar, deren Gleichungen sich durch eine verschwindende Determinante mit zwei Reihen willkürlicher Constanten darstellen. Verfügt man über die letzteren derart (§§. 1, 7 der Abh.), dass man sie aus den Coefficienten zweier Formen $F^{n+r}(\lambda)$, $F^{n+s}(\lambda)$ linear zusammensetzt, deren rte bezw. ste Polaren jene $n-3$ Formen f sind, so erniedrigt sich wiederum die Ordnung der Büschel für ein gegebenes Paar r, s auf $n-r-s-4$, und zwar im äussersten Fall, weil im Allgemeinen $r, s \leqq \frac{1}{3}(n-4)$ ist, auf $\frac{1}{3}(n-2)$ bezw. $\frac{1}{3}(n+1)$ und $\frac{1}{3}n$. Für besondere f kann indessen die Ordnung der erzeugenden Büschel noch weiter herabsinken; die Curven sind dann specieller Natur. Neben Ebenenbüscheln betrachtet Stahl auch die zur Curve perspectiven Regelflächen, die durch den Schnitt der Büschel entstehen. Sie existiren in allen Ordnungen $n-r-2$, wenn $-1 < r < n-4$; im Falle der allgemeinen Curve ist die Ordnung der niedrigsten gleich $\frac{2}{3}(n-1)$ bezw. $\frac{2}{3}(n+1)$ und $\frac{2}{3}n$. Auf den Erzeugenden dieser Regelflächen liegen wieder die Punkte perspectiver Ordnungscurven, u. s. w. Die Forderung, dass diese Curven eben seien, eröffnet neue Gesichtspunkte, die zur Ermittelung von mehrfachen Tangentialebenen der Regelflächen führen.

Wir haben hiermit die Richtung bezeichnet, in denen die genannten Arbeiten sich bewegen; die Fülle der Einzelergebnisse anzuführen, müssen wir uns versagen.

In einer seiner letzten Arbeiten bemerkt Stahl, dass seine „analytischen Operationen meist auf synthetischen Ueberlegungen beruhen“. Dieses Wort ist bezeichnend für alle seine algebraisch-geometrischen Abhandlungen. Häufig und in unregelmässiger Folge wechseln die Beweismittel, und so leidet zuweilen die Einheitlichkeit und Uebersichtlichkeit der Darstellung, sie wird unnötig schwer, wo eine Andeutung des vielleicht fernab liegenden Beweisgrundes den Leser leicht orientiren könnte. Stahl scheint vorauszusetzen, dass jeder, der seine Arbeit liest, die einschlägige Litteratur völlig beherrscht; selbst ungebräuchliche Bezeichnungen, die er irgend einem seiner Vorgänger entlehnt, zu erklären, hält er für unnötig. Aber doch entbehrt seine Darstellung keineswegs der Eleganz und zumal nicht jener Anmut, die Zurückhaltung und anspruchslose Kürze immer begleitet.

Mitten ans dem intensivsten Schaffen, das in stets aufsteigender Linie sich immer schwierigeren Fragen zuwandte, ist Stahl der Wissenschaft entrissen worden, die von ihm Wertvolles noch erwarten durfte. In seinem Nachlasse befindet sich der Entwurf zu einem Buche, das eine zusammenhängende Theorie der rationalen Curven zu geben bestimmt war. Es sollte aus der umfangreichen Litteratur über den Gegenstand das Wichtigste herausheben und unter einheitlichem Gesichtspunkt darstellen. Ein dankenswertes Unternehmen! Und Stahl wäre bei seiner umfassenden Sachkenntnis, seiner Herrschaft über die Hülfsmittel, bei seiner Objectivität und seiner Arbeitskraft dem Thema gewachsen gewesen, wie nicht leicht ein Anderer. Aber so, wie das Werk im Manuscript vorliegt: verschiedenen Zeiten und Auffassungen entsprossen, ungleich in der Behandlung, vielfach durch Neueres, sogar durch Stahl's eigene Arbeiten überholt, wäre dessen Veröffentlichung als Ganzes wohl nicht im Sinne des Autors gelegen. Mehr als einmal scheint ihm die Abfassung dieses Buches, wenn er in der Litteratur eine Lücke vorfand, den Anlass zu eigenen Publicationen gegeben zu haben. So ist das Stück geistiger Arbeit, das in dem Werke niedergelegt ist, der Wissenschaft nicht verloren gegangen.

Strassburg und Tübingen, im Januar 1895.

Wilhelm Ligowski †.

Prof. Dr. Wilhelm Ligowski, geboren am 10. August 1821 zu Borken in Westfalen, trat, nachdem er die Militär-Erziehungsanstalt zu Annaburg durchgemacht hatte, bei der Artillerie ein. Seine mathematische Begabung machte sich geltend, als er, nach seiner Beförderung zum Oberfeuerwerker, zur Artillerie-Prüfungs-Commission commandirt wurde. Der Vorsitzende dieser Behörde, General Neumann, verschaffte ihm die Gelegenheit, Mathematik an der Berliner Universität zu studiren. Nachdem Ligowski einige Jahre hindurch Privatunterricht in der Mathematik gegeben, wurde er 1854 für das Fach der Mathematik als Lehrer an der Königlichen Artillerie- und Ingenieurschule zu Berlin, 1856 zugleich als Lehrer an dem Königlichen Seecadetten-Institut angestellt. Als das letztere Institut, das den Namen einer Königlichen Marineschule erhielt, nach Kiel verlegt wurde, siedelte er 1868 dorthin über. Noch 24 Jahre hindurch wirkte er mit grosser Pflichttreue in Kiel, seit 1872 auch als Lehrer an der neugegründeten Kaiserlichen Marineakademie, mit der die Marineschule verbunden wurde. Im Jahre 1892 nahm er, da seine Gesundheit zu wanken begann, seinen Abschied. Am 8. Dezember 1893 erlag er in Kiel einem Herzleiden.

Ligowski hat in kleineren Abhandlungen eine Reihe mathematischer Einzelfragen behandelt, teils aus der Analysis, teils aus der angewandten Mathematik, der Ballistik und der Nautik. Ausserdem rühren von ihm zwei sehr brauchbare, in mehreren Auflagen erschienene Taschenbücher der Mathematik und der Mechanik her, welche in knapper Form und übersichtlicher Anordnung die wichtigsten Formeln, Sätze und Tabellen enthalten. Er hat sich ferner ein Verdienst um die mathematische Wissenschaft dadurch erworben, dass er Tafeln für die Hyperbelfunctionen, d. h. für die Ausdrücke $\frac{e^x + e^{-x}}{2}$ und $\frac{e^x - e^{-x}}{2}$, berechnete und hiermit die Durchführung einer Anzahl von Aufgaben, die auf jene Functionen zurückkommen, erheblich erleichterte. Das tüchtige und zielbewusste Wirken des Verstorbenen, der aus eigener Kraft zu wissenschaftlicher Stellung aufgestiegen ist, wird ihm überall das ehrenvollste Andenken sichern.

Nachruf für Professor Dr. Julius Worpitzky.

Von

E. Lampe.

Am 4. März 1895 verschied nach langen und schweren Leiden Professor Dr. Julius Worpitzky.

Geboren am 10. Mai 1835 zu Karlsburg in Pommern, besuchte er das Gymnasium zu Anklam und erwarb dort zu Ostern 1855 das Reifezeugnis. Während der fünf ersten Semester studirte er auf der Universität Greifswald, im sechsten Semester (Winter 1857/58) in Berlin. Es folgte nun eine Periode seiner Thätigkeit als Privatlehrer, aus welcher Zeit sein Aufenthalt in Livland (1860/62) hervorzuheben ist. Von dort nach Preussen zurückgekehrt, trat er nach bestandenem Examen pro facultate docendi in das Schellbach'sche Seminar ein (1862/63) und nahm Anteil an der Herausgabe von Schellbach's „Lehre von den elliptischen Integralen und den Thetafunctionen", für welche er, wie in der Vorrede berichtet ist, den Nachweis für die Realität der Wurzel einer grundlegenden Gleichung führte. Bald nachher (1864) wurde er als ordentlicher Lehrer am Friedrichs-Gymnasium angestellt, das damals unter Krech's Leitung mit dem Friedrichs-Realgymnasium vereinigt war, und vier Jahre später wurde er der Nachfolger des jetzigen Stadtschulrats von Berlin, des Geheimen Regierungsrats Professor Dr. Bertram, als erster Mathematiker am Friedrichs-Werderschen Gymnasium, nachdem er ein Jahr vorher in Jena auf Grund seiner Abhandlung „Ueber die Endlichkeit von bestimmten Integralen und Reihensummen" zum Doctor promovirt war. Im Herbste 1872 wurde ihm an der Königlichen Kriegsakademie eine Lehrstelle für Mathematik übertragen. Das grosse Vertrauen, welches die vorgesetzten Behörden in ihn setzten, bekundete sich unter anderem auch darin, dass er für einige Zeit als Hülfsarbeiter in das Ministerium berufen wurde. In der Doppelstellung als Lehrer am Friedrichs-Werderschen Gymnasium und an der Kriegsakademie hat er bis zu seinem Ende treu gearbeitet; doch war er während der letzten drei Jahre seines Lebens durch eine fortgesetzte Folge verschiedener Krankheiten heimgesucht, sodass er bei der allmählichen Zerstörung seiner sonst rüstigen Kräfte in dieser Zeit nur noch wenig leisten konnte. Die Versetzung in den Ruhestand hatte er beim Magistrate von Berlin zum 1. April 1895 erbeten und erhalten. An der Königlichen Kriegsakademie versuchte er seit dem ersten October vorigen Jahres seinen

dreistündigen Vortrag über Mechanik wieder aufzunehmen; vier Monate hat er ihn ohne Unterbrechung mit Aufbietung aller Energie gehalten. Zuletzt versagten aber beim Vortrage die Kräfte. Nach mehrwöchentlichem Krankenlager ist er einem Anfalle der Influenza erlegen, die ihn schon in den vorangehenden Jahren regelmässig ergriffen und jedesmal aufs äusserste geschwächt hatte.

Der Umstand, dass Worpitzky seine Studien hauptsächlich unter der Leitung des bejahrten Grunert in Greifswald gemacht hat, dass er dann mehrere Jahre fern von der Berührung mit jüngeren Mathematikern gelebt hat und in seiner Fortentwickelung auf sich selbst angewiesen gewesen ist, dürfte manches in der Eigenart seines Wesens und seiner Schriften erklären. Seine Arbeiten zeigen ein von angeborenem Talente getragenes, von Erfolg begünstigtes, zielbewusstes und selbständiges Streben, bekunden den heiligen Ernst seiner Forschung, verraten aber auch an manchen Stellen den selbstbewussten Autodidakten. Er besitzt keine Scheu vor Autoritäten, sondern tritt ihnen kühn entgegen, wenn seine eigene, durch ernstes Nachdenken gewonnene Ueberzeugung gegen ihre Lehren streitet; andererseits kann man bei ihm die Berücksichtigung der Schöpfungen seiner Vorgänger vermissen und einen Mangel an Vertiefung in die Leistungen derselben oder an liebevollem Eingehen auf ihre Denkarbeit beklagen. Die Grundbegriffe der Mathematik prüft er mit philosophischem Blicke und kommt daher von selbst dazu, sich angelegentlich mit philosophischen Fragen zu beschäftigen. Diese Eigenschaften verleihen seinen Veröffentlichungen, besonders aber seinen „Elementen der Mathematik“, ihren eigentümlichen Reiz und haben ihnen viele Anerkennung verschafft, aber auch lebhaften Widerspruch hervorgerufen. Jedenfalls haben diese Elemente keine grössere Verbreitung als Lehrbücher zum Unterrichte auf Schulen gefunden. Gerade der philosophische Anstrich derselben und die nicht immer leicht durchsichtige, obschon wohl überdachte, etwas fremdartige Fassung der Sätze haben die Lehrerwelt abgehalten, sie den Schülern in die Hand zu geben. Zum Zwecke der Belehrung für die Lehrer sollten sie in den Schulbibliotheken jedoch vorhanden sein.

In Uebereinstimmung mit dem Charakter seiner Schriften ging Worpitzky bei seiner Lehrthätigkeit vor allem darauf aus, seinen Schülern den folgerichtigen Zusammenhang des Aufbaus der Mathematik zu einem streng logischen System klar zu machen; die Fertigkeit im Lösen von Aufgaben suchte er nur in soweit zu fördern, als dadurch jener höhere Zweck dem Schüler näher geführt wurde, eine Ansicht,

über die er mit Schellbach sich nicht einigen konnte. Dieses Ziel wird auf Schulen meistens wohl nur bei einer kleinen Anzahl von Schülern zu erreichen sein, obwohl es in der That das Ideal eines auf wissenschaftlicher Grundlage beruhenden mathematischen Unterrichtes ist, und sicherlich wird der darauf ausgehende Lehrer stets seinen Schülern Hochachtung vor der ersten sich vor ihnen entfaltenden reinen Wissenschaft einflössen. Wenn von Seiten des Lehrers dann noch jugendliche Begeisterung für seinen Stoff hinzutritt, so wird er gewiss erfreuliche Erfolge erzielen. An der Königlichen Kriegsakademie, wo der Schreiber dieser Zeilen während zwanzig Jahre als College des Verstorbenen Gelegenheit hatte, sein Wirken zu beobachten, hat Worpitzky in der That ein ihn beglückendes Verständnis für seine Vortragsweise gefunden.

Wie die nachfolgende Liste der Veröffentlichungen zeigt, bewegen sich die wissenschaftlichen Abhandlungen Worpitzky's auf dem Gebiete der Functionentheorie, und er begegnet sich bei seinen Untersuchungen öfter mit Briot und Bouquet; hierauf pflegte er in der Unterhaltung gern hinzuweisen, um die Priorität mancher Ergebnisse für sich in Anspruch zu nehmen, wie dies bei der Eigenart seiner Arbeit sehr wohl glaublich war. Hier sei dieser Umstand nur erwähnt, um damit zu zeigen, dass er mit seinen Arbeiten mitten im Gedankenkreise der schöpferischen Mathematiker stand. Sein reichhaltiges Lehrbuch der Differential- und Integralrechnung hat, wie die Elemente der Mathematik, reichlich Lob von der einen Seite, Tadel von der anderen erhalten, verdient aber wegen vieler Vorzüge eine grössere Verbreitung, als es gefunden hat. Denn das Ansehen auch dieses Buches hat unter der eigentümlichen Form gelitten: es soll nicht den Vortrag begleiten, sondern nach Beendigung desselben zur Wiederholung den ganzen Inhalt in logischem Zusammenhange, daher vielfach in ganz anderer Folge vorführen, als dies bei einem ersten Vortrage geschehen kann. So wird die Integration gleichzeitig mit der Differentiation behandelt, und auch dieses grösste und bedeutendste Werk des Dahingeschiedenen zeigt somit überall die selbständige Eigennatur seines Verfassers.

In den letzten Jahren seines Lebens verlangte seine Doppelstellung als Lehrer zweier Anstalten den vollen Aufwand seiner allmählich sich erschöpfenden Kräfte. Noch auf dem letzten Krankenlager entwarf er jedoch Pläne für weitere wissenschaftliche Arbeiten, die er in der Musse des Ruhestandes ausführen wollte. Er wusste nicht, dass der Todesengel schon seine Schatten über ihn breitete, während er über seine

neuen Entwürfe sann. Langsam schwanden seine Kräfte, bis er entschlummerte. Mit ihm ist eine bedeutende Persönlichkeit aus dem Kreise der Berliner Lehrer geschieden.

Ehre seinem Andenken!

Liste der Veröffentlichungen von **Worpitzky.**

I. Bücher.

1. Elemente der Mathematik für gelehrte Schulen und zum Selbststudium. Berlin, Weidmann.
   Erstes Heft: Die Arithmetik. 1872.
   Zweites Heft: Algebra, Combinationslehre nebst Wahrscheinlichkeitsrechnung, Kreisfunctionen nebst Trigonometrie. 1874.
   Drittes und viertes Heft: Planimetrie. 1874.
   Fünftes Heft: Stereometrie. 1883.
2. Lehrbuch der Differential- und Integralrechnung. Berlin, Weidmann. 794 S. gr. 8°. 1880.

II. Abhandlungen.

1. Beitrag zur Integration der Riccati'schen Gleichung. Greifswald, 1862.
2. Ueber die Entwickelung der monodromen und monogenen Functionen durch Kettenbrüche. Erste Folge. Progr. Friedr.-Gymn. Berlin, 1865.
3. Ueber die Endlichkeit von bestimmten Integralen und Reihensummen. Jenenser Inaug.-Diss. Berlin, 1867.
4. Beiträge zur Functionentheorie. Progr. Fr.-Werd. Gymn. Berlin, 1870.
5. Ueber das bestimmte Integral $\int_0^{2\pi} \frac{d\varphi}{A + B\cos\varphi + C\sin\varphi}$, in welchem A, B, C beliebige (reelle oder complexe) Constanten sind. Archiv für Math. u. Phys. LV, 59—64; 1873.
6. Ueber die Grundbegriffe der Geometrie. Archiv für Math. u. Phys. LV, 405—421; 1873.
7. Auswertung des Integrals $\int_0^{\infty} \frac{x^{\alpha-1}}{x+\mu} dx$. Zeitschr. für Math. u. Phys. XIX, 90—92; 1874.
8. Ueber die Wurzeln der Gleichungen. Berlin; 1877.
9. On the roots of equations. Analyst. V, 51—52; 1878.
10. Ueber die Verallgemeinerung der partiellen Integration. Zeitschr. für Math. u. Phys. XXIII, 407—408; 1878.
11. Zahl, Grösse, Messen. Festschr. Friedr.-Werd. Gymn. 16 S. 8°; 1881.
12. Studien über die Bernoulli'schen und Euler'schen Zahlen. Journ. für die reine u. angew. Math. XCIV, 203—233; 1883.
13. Ueber die Partialbruchzerlegung der Functionen, mit besonderer Anwendung auf die Bernoulli'schen. Zeitschr. für Math. u. Phys. XXIX, 45—54, 1884.

14. Ueber die ganzzahlige Bestimmung von $\sqrt{b^2-a^3}$ und $\sqrt[3]{b+\sqrt{b^2-a^3}}$ bei der Auflösung der cubischen Gleichungen. Zeitschr. für math. u. naturw. Unterricht XVI, 578—582; 1885.
15. Ueber die pythagoreischen Dreiecke. Ebenda XVII, 256; 1886.
16. Zur Aufstellung quadratischer Gleichungen $x^2 \pm ax \pm b = 0$, deren Wurzeln bei jeder Combination der Vorzeichen von a und b rational sind. Ebenda XVII, 257, 499—501; 1886.
17. Ueber die realen Lösungen der Gleichung $a^\alpha = b^2 + c^2$. Ebenda XVIII, 168—177; 1887.

Carl Prediger.

Von

Fr. Meyer.

Das Leben des am 19. März 1895 in Clausthal unerwartet Dahingeschiedenen bietet trotz seines äusserlich so einfachen Verlaufes manche Eigentümlichkeiten dar.

Prediger, am 15. November 1822 als Sohn eines Pochsteigers zu Clausthal geboren, besuchte drei Jahre lang (Mich. 1841 bis Mich. 1844) die Bergschule daselbst. Von März 1843 bis December 1848 wurde er in verschiedenen Gruben als Arbeiter beschäftigt.

Inzwischen bestand Prediger (1846) die Prüfung als Markscheidereleve. Durch seine Eigenart zog er die Aufmerksamkeit der Behörde auf sich, so dass er der Forstverwaltung als Geometer überwiesen wurde und einige Jahre darauf auch den Unterricht im Planzeichnen und der descriptiven Geometrie an der Bergschule erhielt.

Eine schöne Frucht der anhaltenden Arbeiten dieser Jahre ist die allseitig als Musterwerk anerkannte Karte vom nordwestlichen Harzgebirge, im Massstabe 1 : 50000. Trotz einiger Vorarbeiten von Gauss war doch noch eine höchst sorgfältige Triangulation nötig, um der — zudem von Römer und Streng geognostisch colorirten — Karte ihren wissenschaftlichen Wert zu verleihen.

Bei Gelegenheit seiner umfassenden Thätigkeit als Geometer wurde Prediger zu manchen Verbesserungen in der Handhabung der Messapparate geführt; er stellte auch Untersuchungen an über die Fehler, welchen man beim Zulegen mit dem Compass ausgesetzt ist.

Gerade diese theoretischen Studien zeigten ihm aber die Unentbehr-

lichkeit der höheren Mathematik, und ungesäumt warf er sich, trotzdem er kein Jüngling mehr war, auf deren Studium.

So darf es denn nicht überraschen, dass er 1863 zum Professor der höheren Mathematik und darstellenden Geometrie an der Clausthaler Bergakademie ernannt wurde. Hunderte von Zuhörern haben bezeugt, mit welchem Geschick und welcher Aufopferung er sein Amt verwaltet hat.

Zunächst für seine Zuhörer liess er eine „Analytische Geometrie der Ebene“ (autographirt), sowie eine „Analytische Geometrie des Raumes“ (bei Löwe, Clausthal 1878) erscheinen. Besonders bei dem letzteren Buche, das einen höheren Standpunkt einnimmt und mit vorzüglichen Abbildungen geschmückt ist, bleibt es zu bedauern, dass es so geringe Verbreitung gefunden hat.

Auch nach seinem Abschiede 1888 gönnte er sich keine Ruhe; er bereitete eine Schrift zur Veröffentlichung vor, welche für eine grosse Anzahl von trigonometrischen Punkten die Umrechnung der alten (Gauss'schen) Coordinaten in die neueren geographischen enthalten sollte. Seine Berechnungsmethoden waren so vielseitig und exact, dass es ihm vielfach gelang, Fehler richtig zu stellen, welche hochberühmte Rechner (Gauss, Encke, Bessel u. A.) begangen hatten.

Er war eine von den seltenen Naturen, die Goethe eine Persönlichkeit nennt.

Auf ihn passt so recht das Wort des Psalmisten: sein Leben war köstlich, denn es ist Mühe und Arbeit gewesen.

Ernst Ritter †.

Aus New-York kommt die Trauernachricht, dass unser Mitglied Ernst Ritter daselbst den 22. September 1895 am Typhus gestorben ist. Erst seit zwei Semestern in Göttingen habilitirt, hatte er einen Ruf an die Cornell University in Ithaca erhalten, den er um so lieber angenommen hatte, als es sich um eine grosse, rein wissenschaftliche Lehraufgabe handelte, vermöge deren die Cornell University an die Seite der anderen mathematisch voranschreitenden grossen amerikanischen Universitäten treten sollte. Bei der Bestimmtheit und Klarheit sowie dem ausgedehnten Wissen, über welche Ritter verfügte, schien er

zur Bewältigung einer derartigen Aufgabe vor anderen besonders geeignet. Es hat anders kommen sollen. Ritter fühlte sich bereits unwohl, als er vor nun vier Wochen die Reise nach Amerika antrat, legte dem aber bei seiner kräftigen Constitution keine Bedeutung bei; er ist dann gleich bei seiner Ankunft in New-York in das Government Hospital auf Ellis Island (einer kleinen Insel im New-Yorker Hafen) aufgenommen worden und hat dort geendet, — angesichts des neuen Continents, umgeben von aller Sorgfalt, welche befreundete amerikanische Mathematiker ihm erweisen konnten.

Ernst Ritter ist in Waltershausen (Thüringen) am 9. Januar 1867 geboren, hat das Gymnasium in Gotha, welches er von Quarta an besuchte, Ostern 1885 absolvirt und folgeweise zuerst 2 Jahre in Jena, dann 4 Jahre in Göttingen studirt. Herbst 1890 absolvirte er das Staatsexamen, Ostern 1891 das Doctorexamen. Die beiden für Lehramtscandidaten in Preussen neuerdings vorgeschriebenen Seminarjahre hat er, vom Herbst 1891 beginnend, in Cassel und Frankfurt abgelegt. Herbst 1893 kehrte er nach Göttingen zurück, zunächst als Assistent am mathematischen Institut daselbst, um sich Ende Sommer 1894 zu habilitiren.

Abgesehen von einer Untersuchung über die Bewegung zweier Massenteilchen nach dem Weber'schen Gesetz, die in Schlömilch's Zeitschrift Bd. 37 publicirt ist, beziehen sich die sämtlichen Arbeiten Ritter's auf die Theorie der automorphen Functionen. Ich nenne hier insbesondere die drei grossen Abhandlungen in den Bänden 41, 44 und 45 der Mathematischen Annalen, denen noch eine vierte Arbeit in Band 47 folgen soll. Ritter hat in denselben eine neue functionentheoretische Grundlegung der genannten Theorie unternommen, wobei er sich, was die Ansätze angeht, an die früher von mir gemachten Vorschläge anschliesst, aber sehr viel mehr in die genaue Durcharbeitung der Einzelheiten eindringt, als vor ihm geschehen war. Kein Zweifel, dass vermöge seiner überaus zuverlässigen Darstellung die allgemeine Theorie der auf einer Riemann'schen Fläche existirenden Functionen eine bleibende Förderung erfahren hat. Ich nenne hier nur den durchgängigen Gebrauch der homogenen Variablen, die multiplicativen Formen, die Stetigkeit der Functionen bei stetiger Abänderung der Riemann'schen Fläche, und aus seiner noch ungedruckten Arbeit die allgemeinen Sätze über die zu einer Riemann'schen Klasse gehörigen linearen Differentialgleichungen.

Der Geist der Strenge und der Besonnenheit, der uns aus diesen

Entwickelungen entgegentritt, ist Ritter nach allen Richtungen zu eigen gewesen und hat sich von je glänzend bewährt: ich erfahre, dass Ritter von Beginn seiner Schulzeit an immer der Erste in seiner Klasse war, wie er denn die Examina an unserer Universität gleichförmig in allen Fächern in einer kaum je dagewesenen glänzenden Weise absolvirt hat.

Ehre seinem Andenken!

Göttingen, den 25. September 1885. F. Klein.

F. E. Neumann.

Von

A. Wangerin.

Am 23. Mai 1895 starb hochbetagt zu Königsberg i. Pr. F. Neumann, der erste und seiner Zeit der hervorragendste Vertreter der theoretischen Physik in Deutschland. Da seine hauptsächlichsten Arbeiten in den Kreis der Disciplinen fallen, deren Pflege die Deutsche Mathematiker-Vereinigung sich zur Aufgabe gestellt hat, so dürfte es angemessen sein, seiner auch an dieser Stelle zu gedenken und seine wissenschaftlichen Leistungen kurz zu schildern. Dabei soll, dem Interesse der meisten Leser des Jahresberichtes entsprechend, auf die rein mathematischen Arbeiten Neumann's etwas ausführlicher eingegangen werden.

Franz Ernst Neumann, am 11. September 1798 zu Joachimsthal in der Uckermark als Sohn eines Landmanns geboren, wurde von seinem neunten Jahre an in Berlin erzogen und besuchte dort das Werder'sche Gymnasium. Schon den Knaben beseelte, wie später den Mann und Greis, eine glühende Vaterlandsliebe; diese trieb ihn dazu, 1815 im Alter von 16 Jahren als freiwilliger Jäger in das Colberger Regiment zu treten. In der Schlacht bei Ligny wurde er durch eine den Oberkiefer, die Zunge und die Oberlippe durchbohrenden Schuss schwer verwundet, jedoch durch die ihm in Düsseldorf zuteil gewordene sorgfältige Behandlung geheilt, so dass er nach sechs Wochen zum Heere und mit diesem später in die Heimat zurückkehren konnte. Hier besuchte er aufs neue das Gymnasium und studirte dann, einem Wunsche seines Vaters folgend, von 1817 an in Berlin und Jena Theologie. 1819 gab er dieses Studium auf und wandte sich in Berlin den Naturwissenschaften, zu denen ihn seine Neigung zog, insbesondere der Mineralogie zu. Daneben studirte er privatim Mathe-

matik. Diese Zeit war für Neumann eine äusserst harte und entbehrungsreiche. Fast von allen Mitteln entblösst, musste er sein Leben aufs kümmerlichste fristen. Aber keine Entbehrung lähmte sein wissenschaftliches Streben. Eine kleine Besserung dieser Verhältnisse trat ein, als sein Eifer, seine Fähigkeiten und seine wissenschaftlichen Erfolge die Aufmerksamkeit seines Lehrers, des Mineralogen Weiss, auf ihn lenkten. Auf Weiss' Veranlassung hielt Neumann 1823 über seine neue Methode der Krystallprojection, der auch seine erste Publication gewidmet war, vor einem auserwählten Kreise von Zuhörern, zu denen u. A. Leopold von Buch gehörte, eine Reihe von Vorlesungen.

Am Ende des Sommersemesters 1825*) bewarb sich Neumann bei der Berliner Philosophischen Facultät um die Promotion. Als Promotionsschrift reichte er eine geometrische Abhandlung ein, auf deren Inhalt weiter unten eingegangen werden soll. Diese Arbeit, die Weierstrass gesprächsweise in den siebenziger und achtziger Jahren wiederholt als eine ausgezeichnete, noch für die Jetztzeit wertvolle Leistung bezeichnete, fand seitens der Facultät nicht die Anerkennung, die sie verdiente. Das Urteil von Dirksen lautete: „dass der Gegenstand der Dissertation und die darin befolgte Methode, beide, mit Rücksicht auf ihre Bedeutsamkeit einer früheren Periode der Wissenschaft angehören, der jetzigen Richtung der Mathematik und dem Bedürfnis eines Physikers . . . so fremd sind, dass ich nicht einsehe, wie der Verfasser . . . einen so unzeitigen Stoff hat wählen und sich so ganz auf den Tummelplatz angehender Gymnasiallehrer hat zurückwerfen können. Zu Vieta's Zeiten hätte die eingereichte Arbeit allerdings ihren grossen Wert gehabt". . . . Trotz dieser Beurteilung wurde die Dissertation nicht zurückgewiesen, ihr Verfasser vielmehr zur mündlichen Prüfung zugelassen, die er am 5. November 1825 bestand. Das Gesamturteil fasste der Dekan in die Worte zusammen: „dass der Candidat seine Würdigkeit, das testimonium doctrinae zu erhalten, besonders durch seine gründlichen physikalischen Kenntnisse, aufs ehrenvollste bekundet habe". Nach bestandenem Examen erklärte sich Neumann freiwillig bereit, statt der nicht ganz gebilligten mathematischen eine andere Abhandlung einzuliefern. Nach Druck der letzteren (De lege zonarum) und gehaltener öffentlicher Disputation wurde er am 16. März 1826 zum Doctor promovirt. Im Herbst desselben Jahres siedelte Neu-

*) Die Nachrichten über Neumann's Promotionsprüfung und über die Beurteilung seiner Promotionsschrift verdanke ich Herrn Prof. H. A. Schwarz, der auf meine Bitte die Güte hatte, die Angaben des Textes aus den Akten der Berliner philosophischen Facultät auszuziehen. Wn.

mann (gleichzeitig mit Jacobi und Dove) als Docent an die Universität Königsberg über und wurde dort 1828 zum ausserordentlichen, 1829 zum ordentlichen Professor der Mineralogie ernannt.

Neben den mineralogischen waren es physikalische Studien, welche Neumann von Beginn seines Aufenthaltes in Königsberg an beschäftigten. Die Frucht dieser Studien waren neben verschiedenen Abhandlungen mineralogischen Inhalts die bahnbrechenden Arbeiten über theoretische Optik und über die Theorie der Elektricität, die er in den dreissiger und vierziger Jahren veröffentlichte, und die ihn bald über die Grenzen Deutschlands hinaus berühmt machten. Auch seine Vorlesungen dehnte er auf das Gebiet der Physik aus und bezeichnete sich später stets als Professor der Physik und Mineralogie. Schon in den zwanziger Jahren hielt er Vorlesungen über die Physik der Erde und die physikalischen Eigenschaften der Mineralien, und von 1830 ab las er ausser über Mineralogie über alle Teile der theoretischen Physik. Diese Vorlesungen, in Deutschland die ersten und lange Zeit die einzigen ihrer Art, haben Jahrzehnte lang zahlreiche Schüler aus allen Theilen Deutschlands, sowie aus der Schweiz und Russland nach Königsberg geführt. Eine Reihe der hervorragendsten Physiker und Mathematiker ist in dieser Schule herangebildet; ich nenne von ihnen nur einige bereits Verstorbene: G. Kirchhoff, Clebsch, Paul du Bois-Reymond, Lothar Meyer. Der Grund für Neumann's Lehrerfolge lag nicht allein in der Klarheit und Anschaulichkeit seines stets auf das sorgfältigste vorbereiteten Vortrags, sondern vor allem darin, dass er es verstand, die Begeisterung, die ihn für seine Wissenschaft erfüllte, auch seinen Zuhörern einzuflössen, und dass er seine Schüler in den von ihm geleiteten seminaristischen Uebungen zu selbständigem Arbeiten anzuleiten wusste. Dafür hingen alle seine Schüler mit der grössten Verehrung an ihm und zollten ihm bleibenden, unauslöschlichen Dank.

War so in Neumann das Ideal eines akademischen Lehrers verkörpert, so nicht minder das eines Gelehrten. Bei seinen Arbeiten war es ihm nicht um Ruhm, um äussere Anerkennung zu thun, sondern lediglich um die Förderung der Wissenschaft. Deshalb legte er, namentlich in späteren Jahren, auch auf die Art der Veröffentlichung der Resultate seiner Forschung wenig Gewicht. Es genügte ihm, diese Resultate durch Mittheilung an seine Schüler und Freunde für die Wissenschaft nutzbar zu machen. So sind manche seiner Entdeckungen erst durch die Arbeiten seiner Schüler oder durch den später erfolgten Druck seiner Vorlesungen weiteren Kreisen bekannt geworden.

Neumann's Tüchtigkeit wurde schon bald nach seiner Uebersiedelung nach Königsberg von seinen dortigen Collegen, insbesondere von Bessel erkannt. Auf Bessel's Befürwortung wurde er verhältnismässig schnell zum Ordinarius befördert und gelangte dadurch in behaglichere äussere Verhältnisse.

Bald wurde er durch seine Arbeiten auch in weiteren Kreisen bekannt; Zeichen der Anerkennung wurden ihm seitens seiner Fachgenossen, Ehrenbezeugungen seitens der Behörden in reichem Masse zu teil. Keine derselben machte ihn stolz, keine vermochte seine wahrhaft rührende Bescheidenheit zu ändern. Schlicht und einfach trat er stets anderen gegenüber auf, einfach war bis an sein Ende seine Lebensweise. In die Oeffentlichkeit trat er selten hinaus, wenn er sich auch für die Entwickelung des Vaterlandes aufs lebhafteste interessirte. Bei den wenigen Anlässen, wo er öffentlich auftrat, zeigte er sich als einen wahren Patrioten im besten Sinne des Wortes.

Der Königsberger Hochschule, zu deren glänzendsten Sternen er zählte, blieb Neumann treu. Bis zum Jahre 1876 setzte er seine Vorlesungen fort. Dann wurde er von der Verpflichtung zu lesen entbunden. Sein wissenschaftliches Interesse erlahmte auch jetzt noch nicht; unermüdlich arbeitete er in seiner Wissenschaft weiter. Eine seltene körperliche und geistige Frische blieb ihm unter der sorgsamen Pflege seiner Tochter bis in seine letzten Lebensjahre bewahrt. Am 23. Mai 1895 schloss er, fast 97 Jahre alt, die müden Augen.

Die erste von Neumann veröffentlichte Arbeit waren seine „Beiträge zur Krystallonomie, erstes Heft*)“, Berlin 1823. Darin entwickelte Neumann eine neue, noch jetzt von den Mineralogen viel benutzte Projectionsmethode der Krystalle. Dieselbe besteht darin, dass man von einem Punkte im Innern des Krystalls auf die sämtlichen Flächen desselben Lote fällt und deren Schnitte mit einer Ebene oder mit einer um den genannten Punkt beschriebenen Kugel bestimmt. Von nicht geringerer Wichtigkeit für die Krystallographie, wie die genannte Arbeit, war seine Dissertation „de lege zonarum principio evolutionis systematum crystallinorum“, Berlin 1826. Hierin wird gezeigt, wie man durch Betrachtung der Zonen (d. i. der Complexe von Flächen, deren Normalen

*) Weitere Hefte sind nicht erschienen.

in einer Ebene liegen) dazu gelangt, aus gewissen Krystallflächen andere abzuleiten und zugleich ihre Indices zu bestimmen.

Dass sich Neumann in der ersten Hälfte der zwanziger Jahre nicht nur mit Anwendungen der Geometrie auf die Krystallographie beschäftigt, sondern daneben auch rein geometrische Studien getrieben hat, zeigt die Arbeit, die er ursprünglich als Promotionsschrift eingereicht hatte. Dieselbe ist im Jahre 1826 in der Oken'schen Zeitschrift Isis (Band XVIII, Heft 4 und 5, p. 349—367, 466—489) abgedruckt und führt den Titel: „De tactionibus atque intersectionibus circulorum et in plano et in sphaera sitorum, sphaerarum atque conorum ex eodem vertice pergentium. Commentatio geometrica auctore Fr. E. Neumann. Berolini, mens Septbr. MDCCCXXV*). Da diese Arbeit wenig bekannt ist, sei es gestattet, auf ihren Inhalt etwas genauer einzugehen. In derselben werden zunächst in höchst eigenartiger Weise die Begriffe der Aehnlichkeitspunkte zweier Kreise, der Potenzlinie derselben, dann die Hauptsätze über Pol und Polare eines Kreises entwickelt, ohne dass jedoch diese Namen gebraucht werden. Den Aehnlichkeitspunkt nennt Neumann: „Punctum analogicum utrique circulo commune in eodem (aut opposito) utriusque latere situm." Auf die Potenzlinie zweier Kreise gelangt er folgendermaassen: Man suche einen Aehnlichkeitspunkt (gleichgültig, welchen) beider Kreise, bestimme die Polaren desselben in Bezug auf jeden der Kreise und nehme endlich die Mittellinie zwischen beiden Polaren. Das ist die Potenzlinie. Als ihre Haupteigenschaft wird hervorgehoben, dass sie alle Kreise, welche die gegebenen berühren, unter gleichen Winkeln schneidet, nämlich unter demselben Winkel, unter dem die beiden Polaren die gegebenen Kreise schneiden. Dieser Eigenschaft wegen wird die Potenzlinie zweier Kreise C', C'' „trajectoria recta circulorum circulos C', C'' tangentium" genannt, während die erwähnten beiden Polaren als „lineae analogicae trajectoriae rectae" bezeichnet wurden. Diesen bei Kreisen auftretenden Begriffen werden jedesmal die analogen Begriffe für Kugeln an die Seite gestellt.

---

*) In der Isis ist als Jahreszahl MDCCCXV angegeben, eine Angabe, die mich früher auf die Vermutung führte, die letzte Ziffer V sei eine verstümmelte X, und die Arbeit sei schon 1820 abgefasst. Dass diese Vermutung eine irrige war, geht daraus hervor, dass aktenmässig feststeht, dass die Abhandlung erst am Ende des Sommers 1825 der Berliner Facultät eingereicht ist. Wahrscheinlich ist die Jahreszahl in Folge eines Schreibfehlers Neumann's falsch angegeben. Nach einer Mitteilung des Herrn Prof. H. A. Schwarz enthält Neumann's Eingabe an die Facultät, in der er sich um die Zulassung zur Promotionsprüfung bewirbt, denselben Schreibfehler.

Auf diese Begriffe, resp. die über dieselben abgeleiteten Sätze gestützt, giebt Neumann eine Construction der Aufgabe des Apollonius, die im wesentlichen mit Gergonne's, Neumann damals nicht bekannter, Construction übereinstimmt; sodann eine Construction der Kugeln, welche vier gegebene Kugeln berühren. — Es folgt die Aufgabe, die Kreise zu construiren, welche drei der Grösse und Lage nach gegebene Kreise C', C'', C''' unter drei gegebenen Winkeln α_1, α_2, α_3 schneiden. Die Construction beruht auf folgender Ueberlegung: Sucht man alle Kreise, welche zwei gegebene Kreise unter gegebenen Winkeln gleichartig (eadem ratione) schneiden, so besteht die Enveloppe derselben aus zwei Kreisen; diese beiden einhüllenden Kreise werden von allen jenen schneidenden Kreisen berührt. Zur Lösung der gestellten Aufgabe hat man nur für je zwei der gegebenen drei Kreise die in Rede stehenden Enveloppen zu suchen, die also zusammen aus 6 Kreisen bestehen, und dann die Kreise zu construiren, welche drei der letztgenannten sechs Kreise berühren (die drei anderen werden von selbst berührt). Für die hier benutzten einhüllenden Kreise wird eine elegante Construction angegeben, die darauf hinauskommt, zwei Kreise zu suchen, die einen gegebenen Punkt zum Aehnlichkeitspunkt und eine gegebene Linie zur Potenzlinie haben. — Mit der Erörterung der analogen Aufgabe für den Raum, der Aufgabe nämlich, die Kugeln zu bestimmen, welche vier gegebene Kugeln unter gegebenen (von einander verschiedenen) Winkeln schneiden, schliesst der erste Abschnitt der Arbeit.

Der zweite Abschnitt behandelt die Bestimmung der geraden Kegel, welche drei gegebene gerade Kegel mit demselben Scheitel berühren oder unter gegebenen Winkeln schneiden. Im dritten Abschnitt werden die Aufgaben, welche im ersten in Bezug auf Kreise der Ebene besprochen waren, auf die Kugelfläche übertragen. Der vierte Abschnitt endlich bespricht specielle Fälle der allgemeinen Aufgaben, indem Punkte oder gerade Linien an Stelle der ebenen Kreise, Punkte oder grösste Kugelkreise an Stelle der kleinen Kugelkreise treten.

Zur Würdigung der besprochenen Arbeit muss man erwägen, dass dieselbe im Jahre 1825 vollendet ist, also vor dem Erscheinen der ersten Arbeiten von Steiner*), dass ferner Neumann bei der Abfassung seiner

---

*) Steiner's Abhandlung „Einige geometrische Betrachtungen", Crelle Band I, behandelt in der Einleitung dieselben Begriffe, die Neumann an die Spitze seiner Arbeit gestellt hat. Datirt ist Steiner's Abhandlung vom März 1826.

Abhandlung die Arbeiten der zeitgenössischen französischen Geometer, insbesondere die von Poncelet und Gergonne, nicht gekannt hat. Er sagt in der Einleitung, nachdem er die Autoren des 18ten Jahrhunderts angeführt hat, ausdrücklich, dass ihm weitere Veröffentlichungen über sein Thema nicht bekannt geworden seien. Wollte man aber auch von Neumann's Leistungen das abziehen, was er nur wieder entdeckt hat, so bliebe doch des Neuen und Eigenartigen genug übrig, um das oben erwähnte Urteil von Weierstrass gerechtfertigt erscheinen zu lassen. Zudem ist hervorzuheben, dass Neumann in der Einleitung es als sein leitendes Princip ausspricht, dass man derartige geometrische Aufgaben, wie er sie behandelt, auch geometrisch lösen müsse, dass der Weg der analytischen Behandlung, der von allen Autoren des 18ten Jahrhunderts eingeschlagen sei, ein Umweg und nicht sachgemäss sei. Neumann giebt weiter an, dass es sein Hauptbestreben gewesen sei, die verschiedenen Constructionen von einheitlichem Gesichtspunkte aus abzuleiten. Er erwähnt endlich, dass er seine Arbeit nur als den ersten Teil einer umfassenderen Abhandlung ansehe, in der analoge Aufgaben zu behandeln wären, bei denen Kegelschnitte an Stelle der Kreise, Flächen zweiter Ordnung an Stelle der Kugeln treten. In dem Betonen der Wichtigkeit rein geometrischer Betrachtungen, in der Behandlung einer grösseren Gruppe von Aufgaben nach einheitlicher Methode hat Neumann in Deutschland keinen Vorgänger. Ich stehe nicht an, ihn auf Grund der besprochenen Arbeit als einen Vorläufer von Steiner zu bezeichnen. Wäre Neumann's Arbeit bekannter geworden, so würde sein Name sicher unter denen der Männer genannt, denen wir die Pflege geometrischer Studien in Deutschland verdanken. —

Die geometrischen Studien hat Neumann nicht weiter fortgesetzt, wenigstens hat er weitere geometrische Arbeiten nicht publicirt. Seine nächsten Veröffentlichungen, meist in Poggendorff's Annalen, eine auch in den Abhandlungen der Berliner Akademie erschienen, waren krystallographischen Inhalts. Die Beschäftigung mit den physikalischen Eigenschaften der Mineralien führte Neumann auf das Studium der Physik, speciell der theoretischen Physik, die das Hauptarbeitsgebiet seines Lebens wurde. Grundlegend waren zunächst seine Forschungen in der theoretischen Optik und der Elasticitätstheorie. In seiner „Theorie der doppelten Strahlenbrechung“ (Poggendorff's Annal. XXV. 1832) erweiterte er die Elasticitätstheorie, die bis dahin nur isotrope Medien in den Kreis ihrer Betrachtung gezogen hatte, indem er die allgemeinen Elasticitätsgleichungen für krystallinische Medien aufstellte, die in Bezug

auf drei rechtwinklige Ebenen symmetrisch sind. Auf Grund dieser Gleichungen gab er die erste theoretische Ableitung der Gesetze der doppelten Strahlenbrechung und füllte so eine Lücke in Fresnel's Forschungen aus. Die von Neumann entwickelte Theorie ergab nicht nur die Richtung der von optisch-zweiaxigen Krystallen gebrochenen Strahlen in Uebereinstimmung mit der Erfahrung, sie erklärte auch das Verhalten der gebrochenen Strahlen hinsichtlich ihrer Polarisation. Allerdings waren, um die Theorie mit der Erfahrung in Einklang zu bringen, noch zwei Hülfsannahmen nötig; die erste derselben betraf gewisse Beziehungen zwischen den in den elastischen Gleichungen auftretenden Constanten, die zweite bezog sich auf die Schwingungsrichtung des polarisirten Lichtes, die nach Neumann in der Polarisationsebene liegt, während nach Fresnel's Anschauungen die Schwingungen senkrecht zur Polarisationsebene vor sich gehen.

Welche von diesen beiden Anschauungen den Vorzug verdient, ist Jahrzehnte lang zwischen den Physikern streitig gewesen; ein stichhaltiger experimenteller Nachweis für die Richtigkeit der einen oder der anderen hat sich nicht erbringen lassen. Vielleicht trifft die neuerdings in Aufnahme gekommene elektromagnetische Lichttheorie das Richtige, wenn sie im polarisirten Lichte beide Arten von Schwingungen als gleichzeitig vorhanden annimmt. — Noch ein für die Grundlage der theoretischen Optik wichtiger Punkt sei aus dieser Arbeit hervorgehoben. Neumann erörtert in der Einleitung, weshalb man berechtigt sei, die Lichtschwingungen bei allen Körpern als elastische anzusehen. Er sagt: So lange die Verschiebungen kleiner sind als die Sphäre des stabilen Gleichgewichts, fällt der Unterschied zwischen dem festen, flüssigen und gasförmigen Zustande fort. Für diese Arten der Bewegung gelten also dieselben Gleichungen, welches auch der Cohäsionszustand des Mediums ist.

Dieser für die Ausbildung der Undulationstheorie äusserst bedeutungsvollen Arbeit folgen zunächst mehrere kleinere Abhandlungen optischen Inhalts, in denen u. a. die Erscheinungen des an einer Metallfläche reflectirten Lichtes aus zwei einfachen Grundsätzen abgeleitet werden, in denen ferner der Begriff der optischen Axen eines zweiaxigen Mediums festgelegt und gezeigt wird, dass sich die Fortpflanzungsgeschwindigkeit ebener Wellen eines derartigen Mediums auf sehr einfache Weise durch die Winkel ausdrücken lässt, welche die Wellennormale mit den optischen Axen bildet. Im Jahre 1835 wird dann die grosse Arbeit „Theoretische Untersuchung der Gesetze, nach welchen das Licht an der Grenze zweier vollkommen durchsichtigen Medien reflectirt und gebrochen wird", vollendet

und in der Berliner Akademie vorgetragen (Abhandlungen der Berl. Akademie 1835). Neumann nimmt hier die Aufgabe, die Intensität des an der Oberfläche eines durchsichtigen Mediums reflectirten und gebrochenen Lichtes zu bestimmen, eine Aufgabe, die bis dahin (durch Fresnel) nur für die Brechung an unkrystallinischen Medien behandelt war, in voller Allgemeinheit, d. h. für beliebige durchsichtige Krystalle, in Angriff und löst dieselbe vollständig auf Grund seiner Anschauung über die Schwingungsrichtung des polarisirten Lichtes. Die zum Teil umfangreichen, aber doch durchsichtigen und eleganten Entwickelungen führen zu Gesetzen, welche mit den durch Beobachtung gefundenen übereinstimmen, sowie zu einer Reihe neuer Resultate. Ich erwähne darunter das, welches sich auf die Verteilung des Lichtes in dem durch konische Refraction aus einem eintretenden Strahle entstehenden Lichtkegel und auf die Lage der Polarisationsebene in den einzelnen Seiten des Kegels bezieht. An einer Stelle enthält die Arbeit eine Entwickelung von Jacobi, in der für eine von Neumann durch geometrische Betrachtungen abgeleitete Relation ein analytischer Beweis mitgeteilt wird.

Die experimentelle Prüfung der in der letztgenannten Arbeit gefundenen Resultate gab Neumann zur Abfassung mehrerer kleiner Aufsätze in Poggendorff's Annalen Veranlassung. In einem derselben wird gezeigt, dass die Cauchy'schen Reflexionsformeln der Erfahrung widersprechen, zugleich werden Formeln für die Totalreflexion abgeleitet.

Endlich ist als letzte in der Reihe der optischen Arbeiten Neumann's die über „die Gesetze der Doppelbrechung des Lichtes in comprimirten oder ungleichförmig erwärmten unkrystallinischen Körpern“ (Abhandlungen der Berl. Akad. 1841) zu nennen. In dieser sehr umfangreichen Abhandlung werden zuerst die Gesetze der Doppelbrechung in gleichförmig comprimirten oder dilatirten krystallinischen Medien entwickelt; sodann werden die Farbenerscheinungen abgeleitet, welche ein ungleichförmig dilatirter Körper im polarisirten Lichte zeigt, endlich wird im dritten Teile eine Theorie der Farben aufgestellt, welche in durchsichtigen unkrystallinischen Körpern aus ungleicher Temperaturverteilung entstehen. Zu dem Zwecke werden zunächst die Differentialgleichungen aufgestellt, von welchen das System der durch Erwärmung entstehenden Dilatationen abhängt. Diese Gleichungen waren im Jahre 1838 von Duhamel gefunden; doch giebt Neumann an, dass er schon viele Jahre vor Duhamel's Veröffentlichung im Besitze jener Formeln gewesen sei. Ferner leitet Neumann jene Formeln in viel allgemeinerer Weise her als Duhamel, so nämlich, dass die Ableitung auch für krystallinische Medien gilt. Hat man durch

Integration der in Rede stehenden Gleichungen das System von Dilatationen ermittelt, so führen die im zweiten Abschnitt gefundenen Resultate zur Lösung der Aufgabe. Von der entwickelten allgemeinen Methode wird nun eine Reihe physikalisch und mathematisch interessanter Anwendungen gemacht. In diesen tritt ganz besonders Neumann's Eigenart in der Verbindung von Theorie und Experiment hervor.

Die eben erwähnten Anwendungen beziehen sich auf die vorübergehenden Farben, die in durchsichtigen Körpern durch Erwärmung entstehen. Darüber hinaus aber war Neumann, wie er am Schluss der Einleitung der Arbeit anführt, auch im Besitz der Principien, mittelst deren die bleibenden Farben, welche durch Härtung, durch rasche Abkühlung etc. entstanden sind, auf den Calcül zurückgeführt werden. Er erörtert kurz, wie man zu den Differentialgleichungen gelangen kann, welche die relative Lage der Teilchen in einem durch bleibende Dilatationen gespannten Körper bestimmen, behält jedoch die weitere Entwickelung einer späteren Abhandlung vor. Leider ist dieselbe bisher nicht veröffentlicht. Noch ein Punkt in der hier besprochenen Arbeit verdient Erwähnung. In einer Anmerkung giebt Neumann die Grundzüge einer einfachen Theorie der Dispersion.

In den vierziger Jahren wenden sich Neumann's Arbeiten von dem Gebiete der Optik und Elasticität ab und dem der Elektricität zu. Auch hier waren seine Forschungen epochemachend. Ihm verdanken wir (Abhandl. d. Berl. Akad. 1845, wieder abgedruckt in Ostwald's Klassikern der exacten Wissenschaften Heft 10) die erste theoretische Ableitung der Gesetze der Induction. Das von ihm begründete Elementargesetz der inducirten Ströme ist dauernd mit seinem Namen verknüpft, ebenso ein allgemeines Princip, das er über derartige Ströme in einer weiteren Arbeit (Abh. d. Berl. Akad. 1848, abgedruckt in Ostwald's Klassikern, Heft 36) aufstellte. In der letztgenannten Arbeit begründete er ferner das sogenannte Neumann'sche Potentialgesetz geschlossener elektrischer Ströme. Auch rein experimentell arbeitete er im Gebiete der Elektricität; u. a. rührt von ihm eine neue Methode zur Bestimmung der Polarisation und des Uebergangswiderstandes her.

Eine weitere Gruppe von Arbeiten betraf die Theorie der Wärme, in Sonderheit die Methoden zur Bestimmung der specifischen Wärme. Auch diese Arbeiten sind ein Muster für die Art, wie Theorie und Experiment zu verbinden sind.

Gehören Neumann's wichtigste Leistungen dem Gebiete der Physik, insbesondere der mathematischen Behandlung physikalischer Probleme

an, so hat er doch auch einen Zweig der reinen Mathematik wesentlich gefördert, nämlich die Theorie der Kugelfunctionen. Seine erste darauf bezügliche Arbeit findet sich in Schumacher's „Astronomischen Nachrichten“, Band 15, 1838 (wieder abgedruckt in den Mathem. Annal., Bd. 14, 1879). Dieselbe führt den Titel: „Ueber eine neue Eigenschaft der Laplace'schen $Y^{(n)}$ und ihre Anwendung zur analytischen Darstellung derjenigen Phänomene, welche Functionen der geographischen Länge und Breite sind“. Darin wird die Aufgabe behandelt, in einer endlichen, nach dem Laplace'schen $Y^{(n)}$ fortschreitenden Reihe die Coefficienten so zu bestimmen, dass die Reihe für eine endliche Anzahl von Werthen der unabhängigen Veränderlichen (geographische Länge und Breite) gegebene Werthe annimmt. Diese Aufgabe wird von Neumann viel einfacher gelöst, als es von Gauss in seiner Theorie des Erdmagnetismus für einen speciellen Fall geschehen ist. Während Gauss, der die Entwickelung bis zu den Kugelfunctionen vierter Ordnung incl. führt, zur Bestimmung der erforderlichen 25 Constanten 25 Gleichungen mit 25 Unbekannten auflöst, wird hier eine allgemeine Methode entwickelt, jene Constanten mit leichter Mühe bis zu jeder Ordnung der Kugelfunctionen zu berechnen; dabei wird allerdings vorausgesetzt, dass die Beobachtungsorte nach einem gewissen Gesetze über die Erdoberfläche vertheilt sind. Unter dieser Voraussetzung existirt nämlich ein einfaches System von Factoren, mit denen man nur nötig hat, die Gleichungen zu multipliciren und dann zu addiren, um ohne weiteres die gesuchten Constanten zu finden. Das angedeutete Verfahren beruht auf folgenden, von Neumann aufgestellten Sätzen über endliche Summen von Kugelfunctionen. Man bestimme $2p+1$ Grössen $\mu_1, \mu_2, \ldots, \mu_{2p+1}$ und $2p+1$ andere Grössen $a_1, a_2, \ldots, a_{2p+1}$ so, dass sie den $2p+2$ Gleichungen genügen:

$$\Sigma a_k = 1, \quad \Sigma a_k \mu_k = 0, \quad \Sigma a_k \mu_k^2 = \tfrac{1}{3}, \quad \ldots,$$

$$\Sigma a_k \mu_k^{2p} = \frac{1}{2p+1}, \quad \Sigma a_k \mu_k^{2p+1} = 0,$$

worin alle Summen von $k = 1$ bis $k = 2p+1$ zu nehmen sind: Dann ist

$$\Sigma a_k P_n(\mu_k) P_m(\mu_k) = 0,$$

falls $m \gtrless n$, während für $m = n$

$$\Sigma a_k P_n(\mu_k) P_n(\mu_k) = \frac{2}{2n+1}$$

ist. Durch diese Hülfssätze, die für $p = \infty$ in die bekannten Integralsätze der Kugelfunctionen übergehen, sowie durch zwei analoge, die zu-

geordneten Kugelfunctionen betreffende Sätze gelingt, in Verbindung mit bekannten trigonometrischen Summenformeln, die angestrebte einfache Bestimmung der gesuchten Constanten. — Will man nun die Kugelfunctionenreihe bis $Y^{(p)}$ incl. haben, so dass es sich um die Bestimmung von $(p+1)^2$ Constanten handelt, so bedarf es der Kenntnis der Werte der zu entwickelnden Function für die Durchschnittspunkte von $2p$ äquidistanten Meridianen mit denjenigen Parallelkreisen, für welche μ_1, $\mu_2, \ldots, \mu_{2p+1}$ die Sinus der Breite darstellen. Von diesen Grössen μ sind $2p$ ganz willkürlich. Die Zahl der erforderlichen Beobachtungsdaten, $2p(2p+1)$, reducirt sich auf $p(p+1)$, falls die Grössen $\mu_1, \ldots, \mu_{p+1}$ Wurzeln der Gleichung $P_{p+1}(\mu) = 0$ sind.

Eine zweite Arbeit über Kugelfunctionen hat Neumann im 37. Bande des Crelle'schen Journals (1848) veröffentlicht: „Entwickelung der in elliptischen Coordinaten ausgedrückten reciproken Entfernung zweier Punkte in Reihen, welche nach den Laplace'schen $Y^{(n)}$ fortschreiten etc.". Der durch diese Arbeit angebahnte Fortschritt betrifft drei Punkte. Der wesentlichste von diesen ist die Darstellung der Kugelfunction zweiter Art durch einen geschlossenen logarithmischen Ausdruck, d. h. die Aufstellung der Formel*)

$$Q_n(x) = \int_{-1}^{+1} \frac{P_n(z)dz}{x-z} = R_{n-1} - P_n . \log\left[\frac{x-1}{x+1}\right],$$

wo P_n die Kugelfunction erster Art, R_{n-1} eine ganze Function vom Grade $n-1$ ist. Eine ähnliche Darstellung folgt für die sogenannte zugeordnete (oder nach Neumann's Bezeichnung „adjungirte") Kugelfunction zweiter Art. Nebenbei wird eine Anzahl von Werten der genannten Functionen für specielle Werte des Arguments bestimmt. — Der zweite Punkt betrifft die Potentialaufgaben für Rotationsellipsoide (bei den im Titel erwähnten elliptischen Coordinaten handelt es sich nicht um die allgemeinen elliptischen Coordinaten, sondern nur um solche für Rotationsflächen). Die erwähnte Aufgabe war von Lamé für den Innenraum, von Heine (Dissert. 1842, Crelle J. 26, 1843) für den Aussenraum von Rotationsellipsoiden gelöst. Heine hatte zugleich erkannt, dass die auftretenden Reihen Kugelfunctionen sind. Neumann ist der Erste, der die reciproke Entfernung zweier Punkte entwickelt, d. h. die in den allgemeinen Entwickelungen auftretenden Constanten für diesen speciellen, aber fundamentalen Fall bestimmt hat. Dazu kommt noch eins, und das bildet das dritte erhebliche

*) Neumann's $Q_n(x)$ ist das Doppelte der von Heine mit $Q^n(x)$ bezeichneten Function.

Resultat. Geht man von der transformirten Laplace'schen Gleichung $\Delta V = 0$ aus, so erkennt man, so lange es sich um verlängerte Rotationsellipsoide handelt, leicht, dass an Stelle der bei der Kugel auftretenden negativen Potenzen des Abstandes vom Mittelpunkt hier Kugelfunctionen zweiter Art zu nehmen sind. Für abgekürzte Rotationsellipsoide ist das Gleiche nicht ohne weiteres klar. Vielmehr scheint es, als ob hier Summen von Functionen erster und zweiter Art auftreten können. Neumann deckt (durch Betrachtung der Ableitungen von V nach der Normale des Ellipsoids oder des confocalen Hyperboloids) den Grund auf, aus dem die Entwickelung für abgekürzte Ellipsoide genau dieselbe Form hat wie für verlängerte. Den Schluss der Arbeit bildet eine Anwendung der behandelten Aufgabe auf die Bestimmung des magnetischen Zustandes eines Rotationsellipsoids unter der Einwirkung beliebiger verteilender Kräfte, falls letztere ein Potential besitzen. Diese Aufgabe war vorher von Poisson nur für constante Kräfte gelöst worden.

Eine dritte, die Kugelfunctionen betreffende Arbeit Neuman's, „Beiträge zur Theorie der Kugelfunctionen", ist 1878 als selbständige Schrift erschienen; und zwar ist dieselbe von Herrn C. Neumann nach den Manuscripten seines Vaters veröffentlicht worden. Die Hauptbedeutung dieser Schrift scheint mir in Folgendem zu liegen. Bei den Anwendungen der Kugelfunctionen auf die Potentialtheorie spielen nur diejenigen zugeordneten Kugelfunctionen, d. h. diejenigen Lösungen der Differentialgleichung

$$\frac{d(1-x^2)\frac{dy}{dx}}{dx} + \left\{n(n+1) - \frac{m^2}{1-x^2}\right\} y = 0$$

eine Rolle, für welche der Nebenindex m kleiner oder gleich dem Hauptindex n ist. Die Notwendigkeit dieser Beschränkung ergiebt sich von selbst bei der Entwickelung der durch Polarcoordinaten ausgedrückten reciproken Entfernung zweier Punkte. Anders liegt die Sache, wenn man eine Reihenentwickelung für die Lösung der Laplace'schen Gleichung $\Delta V = 0$ sucht. Hier sieht man den Grund jener Beschränkung nicht a priori ein; wendet man aber trotzdem, wie es manche Autoren, z. B. Lamé, thun, ohne weitere Begründung nur Functionen an, bei denen $m \leq n$ ist, so bleibt in der Ableitung eine wesentliche Lücke*). Diese Lücke nun wird durch Neumann's Beiträge ausgefüllt. Hier werden nämlich die Integrale der obigen Differentialgleichung auch für $m > n$

---

*) Auch bei Heine tritt dieser Punkt nicht deutlich und klar genug hervor.

eingehend untersucht. Es ergiebt sich, dass, während für den Fall $0 < m \leqq n$ eine Particularlösung jener Gleichung existirt, die für die beiden singulären Punkte $x = +1$ und $x = -1$ verschwindet, ein Gleiches für $m > n$ nicht mehr stattfindet. Vielmehr wird hier diejenige Particularlösung, die für $x = +1$ verschwindet, für $x = -1$ unendlich, und umgekehrt. Es folgt dies, wenn man die Lösung der Differentialgleichung in die Form bringt: $\left(\frac{x-1}{x+1}\right)^{\frac{m}{2}} . F$, wo F eine nach Potenzen von $x+1$ fortschreitende Reihe ist. Man könnte wohl anführen, dass sich das erwähnte Verhalten der Integrale obiger Gleichung aus den allgemeinen Eigenschaften der hypergeometrischen Reihe entnehmen lässt. Indessen ist es wichtig, dass für den speciellen Fall jener Reihe, den die Kugelfunctionen darstellen, jene Eigenschaft auch durch specielle, einfache Methoden abgeleitet wird, und das leisten Neumann's Beiträge. Dieselben enthalten eine Anzahl neuer Reihen und Integraldarstellungen einmal der zugeordneten Kugelfunctionen selbst, sodann ihrer Erweiterungen für $m > n$. Daran schliesst sich eine äusserst ausführliche Zusammenstellung von Recursionsformeln, die zwischen Kugelfunctionen mit auf einander folgenden Indices bestehen, und die teils bekannt, zum grossen Teil aber neu sind, und weiter eine Tabelle besonders wichtiger Specialwerte jener Functionen. Endlich wird im zweiten Teile der Beiträge die Aufgabe behandelt, das Product zweier Kugelfunctionen in eine einfache Kugelfunctionenreihe zu entwickeln; auch dabei ergeben sich bemerkenswerte Resultate.

Die eben besprochene Schrift war die letzte Arbeit, welche von Neumann selbst oder nach seinen Manuscripten veröffentlicht ist. Das Bild seiner Leistungen, das ich, zum Teil nur in kurzen Andeutungen, zu entwerfen versucht habe, würde aber ein unvollständiges sein, wenn ich nicht noch der Ausarbeitung und Herausgabe von Neumann's Vorlesungen durch mehrere seiner Schüler gedächte. Enthalten diese Vorlesungen doch so manches Resultat von den Forschungen des Meisters, und haben sich dieselben doch, trotzdem sie verhältnismässig spät gedruckt sind, einen weiten Leserkreis erworben. Bisher sind die folgenden Vorlesungen erschienen:

1. Theorie des Magnetismus, herausgegeben von C. Neumann, 1881.
2. Einleitung in die theoretische Physik, herausgegeben von C. Pape, 1883.
3. Elektrische Ströme, herausgegeben von K. Von der Mühll, 1884.
4. Theoretische Optik, herausgegeben von E. Dorn, 1885.
5. Theorie der Elasticität fester Körper und des Lichtäthers, herausgegeben von O. E. Meyer, 1885.

6. Theorie des Potentials und der Kugelfunctionen, herausgegeben von C. Neumann, 1887.
7. Theorie der Capillarität, herausgegeben von A. Wangerin, 1894.

Es würde zu weit führen, auf den Inhalt der Vorlesungen hier näher einzugehen. Ich muss in dieser Beziehung sowie hinsichtlich mancher Punkte, die ich nur kurz berühren konnte, auf die „Erinnerungen an F. E. Neumann“ von Herrn W. Voigt (Nachrichten der Gesellschaft der Wissenschaften zu Göttingen, Math.-Phys. Kl., 1895 Nr. 2), sowie auf die soeben von Herrn P. Volkmann veröffentlichte Schrift (Franz Neumann, Leipzig, B. G. Teubner, 1896) verweisen.

Halle a. S., December 1895.

Bericht
über die wissenschaftlichen Sitzungen
der Deutschen Mathematiker-Vereinigung
während der Jahres-Versammlung zu Wien.

Riemann und seine Bedeutung für die Entwickelung der modernen Mathematik.*)

Von

F. Klein.

Hochgeehrte Anwesende!

Es hat gewiss seine ganz besondere Schwierigkeit, über mathematische Dinge, oder auch nur über allgemeine Verhältnisse und Beziehungen innerhalb der Mathematik vor einem grösseren Publicum zu sprechen. Diese Schwierigkeit resultirt daraus, dass die Begriffe, mit denen wir uns beschäftigen und deren inneren Zusammenhang wir erforschen, selbst erst das Product fortgesetzter mathematischer Gedankenarbeit sind, dass sie dem gewöhnlichen Leben fern liegen.

Trotzdem habe ich nicht angestanden, der ehrenvollen Aufforderung zu entsprechen, welche der Vorstand Ihrer Gesellschaft neuerdings an mich richtete, und den heutigen ersten Vortrag zu übernehmen.

Ich hatte das Beispiel des nun vollendeten grossen Forschers vor Augen, welcher ursprünglich als Redner in Aussicht genommen war. Es ist zweifellos ein grosses Verdienst von Hermann v. Helmholtz, dass er von Beginn seiner Laufbahn bemüht gewesen ist, die Probleme und Resultate der wissenschaftlichen Arbeit auf allen den vielen von ihm berührten Gebieten in allgemein verständlichen Vorträgen dem Kreise der weiteren Fachgenossen vorzulegen; er hat dadurch jeden einzelnen von uns auf dessen eigenem Gebiete gefördert. Wenn es von vorn herein unmöglich scheint, ein Gleiches im Hinblick auf reine Mathematik zu leisten, so drängen dafür die inneren Verhältnisse meines Faches immer zwingender daraufhin, zu versuchen, was sich erreichen lassen möchte. Ich spreche hier nicht als einzelner, ich spreche im Namen der sämtlichen Mitglieder der mathematischen Vereinigung, welche

*) Vortrag gehalten in der öffentlichen Sitzung am Mittwoch, den 26. September 1894.

sich im Anschlusse an die Gesellschaft der Naturforscher und Aerzte vor einigen Jahren gebildet hat, und die, wenn nicht formal, so doch thatsächlich mit ihrer ersten Section identisch ist. Wir empfinden, dass unter dem Einflusse der modernen Entwickelung unsere fortschreitende Wissenschaft je länger je mehr Gefahr läuft, sich zu isoliren. Die enge Beziehung zwischen Mathematik und theoretischer Naturwissenschaft, wie sie zum Segen beider Gebiete seit dem Emporkommen der modernen Analysis bestand, droht zu zerreissen. Hier liegt eine grosse, täglich wachsende Gefahr. Dem wollen wir Mitglieder der mathematischen Vereinigung nach Kräften entgegenwirken. In diesem Sinne war es, dass wir uns an die Naturforscherversammlung angeschlossen haben. Wir wünschen von Ihnen im persönlichen Verkehre zu lernen, wie sich der wissenschaftliche Gedanke in Ihren Disciplinen entwickelt, und wo dem entsprechend der Ansatzpunkt für das Eingreifen des Mathematikers gegeben sein mag. Wir wünschen umgekehrt, von Ihrer Seite für unsere Auffassungen und Bestrebungen einiges Interesse und Verständnis zu finden. In diesem Sinne stehe ich vor Ihnen und versuche, von der Bedeutung desjenigen Forschers ein Bild zu entwerfen, der wie kein anderer für die Entwickelung der modernen Mathematik bestimmend gewesen ist, von Bernhard Riemann. Dabei hoffe ich, jedenfalls denjenigen unter Ihnen einiges bieten zu können, denen die Ideengänge der Mechanik und theoretischen Physik geläufig sind. Sie Alle aber müssen fühlen, dass hier Verbindungspunkte mit dem naturwissenschaftlichen Denken vorliegen.

Der äussere Lebensgang von Riemann wird vielleicht Ihre Teilnahme, aber kaum ihr besonderes Interesse erregen. Riemann ist einer der stillen Gelehrten gewesen, welche ihre tiefen Gedanken langsam in sich ausreifen lassen. Als er 1851 in Göttingen mit einer allerdings sehr hervorragenden Dissertation promovirte, war er 25 Jahre alt; es dauerte weitere drei Jahre, bis er sich ebenda habilitirte. Um diese Zeit entstehen in rascher Aufeinanderfolge alle die bedeutenden Arbeiten, von denen ich zu berichten habe. Riemann ist 1859 nach dem Tode von Dirichlet dessen Nachfolger an der Göttinger Universität geworden, aber schon 1863 begann die unheilvolle Krankheit, der er 1866 zum Opfer gefallen ist, im Alter von nur 40 Jahren. Seine gesammelten Werke, welche zuerst 1876 von Heinrich Weber und Dedekind herausgegeben sind (und die bereits in zweiter Auflage vorliegen), sind nicht etwa besonders umfangreich; sie füllen einen Octavband von ca. 550 Seiten, darunter nur etwa die Hälfte Arbeiten, die zu Riemann's Lebzeiten veröffentlicht worden sind. Die grosse Wirkung, welche von Riemann

ausgegangen ist und fortwährend ausgeht, ist einzig eine Folge der Eigenartigkeit und selbstverständlich der eindringenden Kraft seiner mathematischen Betrachtungen.

Entzieht sich die letztere der heutigen Darlegung, so meine ich die Eigenart der Riemann'schen Mathematik Ihnen allerdings vorweg erklären zu können, indem ich den einheitlichen Grundgedanken bezeichne, von dem aus alle seine Entwickelungen entspringen. Ich darf vorweg erwähnen, dass Riemann sich viel und eingehend mit physikalischen Betrachtungen beschäftigt hat. Aufgewachsen in der grossen Tradition, die durch die Vereinigung der Namen Gauss und Wilhelm Weber bezeichnet ist, beeinflusst andererseits von der Herbart'schen Philosophie, hat er immer wieder daran gearbeitet, in mathematischer Form eine einheitliche Formulirung der sämtlichen Naturerscheinungen zu Grunde liegenden Gesetze zu finden. Diese Untersuchungen sind, wie es scheint, niemals zu einem bestimmten Abschlusse gekommen und liegen uns in Riemann's Nachlass nur ganz bruchstückweise vor. Es handelt sich um verschiedene Ansätze, denen nur dies eine gemeinsam ist, was heute unter der Herrschaft von Maxwell's elektro-magnetischer Lichttheorie die allgemeine Grnndanschauung wenigstens der jüngeren Physiker sein dürfte, die Annahme nämlich, dass der Raum von einer continuirlich ausgebreiteten Flüssigkeit erfüllt ist, welche gleichzeitig der Träger der optischen, wie der elektrischen und der Gravitationserscheinungen ist. Ich verweile nicht bei den Einzelheiten, umsomehr, als dieselben heute nur noch historisches Interesse besitzen dürften. Was ich betonen will, ist dies, dass eben hier die Quelle von Riemann's rein mathematischen Entwickelungen liegt. Was in der Physik die Verbannung der Fernwirkungen, die Erklärung der Erscheinungen durch die inneren Kräfte eines raumerfüllenden Aethers ist, das ist in der Mathematik das Verständnis der Functionen aus ihrem Verhalten im Unendlich-Kleinen, insbesondere also aus den Differentialgleichungen, denen sie genügen. Und wie im übrigen die einzelne Erscheinung im Gebiete der Physik von der allgemeinen Anordnung der Versuchsbedingungen abhängt, so individualisirt Riemann seine Functionen durch die besonderen Grenzbedingungen, die er ihnen auferlegt. Die Formel, deren man zur rechnerischen Beherrschung der Function bedarf, erscheint hier als Schlussresultat der Betrachtungen, nicht als Ausgangspunkt. Wenn ich wagen darf, die Analogie so scharf zu betonen, so werde ich sagen, dass Riemann im Gebiete der Mathematik und Faraday im Gebiete der Physik parallel

stehen. — Diese Bemerkung bezieht sich zunächst auf den qualitativen Inhalt der beiderseitigen Gedankengänge; ich meine aber, dass auch die Wichtigkeit der von den beiden Forschern erreichten Resultate, gemessen an den Bedingungen der einzelnen Wissenschaft, vergleichbar sei.

Indem ich mich jetzt dazu wende, an der Hand der hiermit gegebenen Auffassung mit Ihnen die einzelnen Hauptgebiete von Riemann's mathematischen Untersuchungen zu durchwandern, habe ich selbstverständlich mit derjenigen Disciplin zu beginnen, welche am innigsten mit seinem Namen verbunden erscheint, wenn er sie selbst auch nur als einen Beleg für sehr viel weiter ausgreifende, umfassende Tendenzen betrachten mochte: — mit der Functionentheorie complexer Variabler.

Der fundamentale Ansatz dieser Theorie ist wohlbekannt; bei Untersuchung der Functionen einer Variablen z substituirt man für diese Variable eine zweiteilige Grösse $x+iy$, mit der so gerechnet wird, dass man für i^2 allemal -1 einträgt. Der Erfolg ist, dass die Eigenschaften der Functionen einfacher Variabler, die wir gewöhnlich betrachten, in sehr viel höherem Maasse verständlich werden, als ohne eine solche Maassnahme. Um die eigenen Worte Riemann's aus seiner Dissertation von 1851 zu gebrauchen (in welcher er die Grundlinien für die ihm eigentümliche Behandlungsweise unserer Theorie gezogen hat): es tritt beim Uebergange zu complexen Werten eine sonst versteckt bleibende Harmonie und Regelmässigkeit hervor.

Der Begründer dieser Theorie ist der grosse französische Mathematiker Cauchy*); aber erst in Deutschland hat dieselbe ihr modernes Gepräge erhalten, durch welches sie, so zu sagen, in den Mittelpunkt unserer mathematischen Ueberzeugungen gerückt wird. Das ist der Erfolg der gleichzeitigen Bestrebungen der beiden Forscher, die wir noch wiederholt neben einander zu nennen haben, nämlich von Riemann und andererseits von Weierstrass.

Auf dasselbe Ziel gerichtet, sind die Methoden dieser beiden Mathe-

---

*) Ich sehe bei der Darstellung des Textes von Gauss ab, der, hier wie in anderen Gebieten seiner Zeit vorauseilend, zahlreiche Entdeckungen anticipirt hat, ohne hierüber irgend etwas an die Oeffentlichkeit zu bringen. Es ist besonders merkwürdig, dass man bei Gauss functionentheoretische Ansätze findet, die ganz in der Richtung der späteren Riemann'schen Methoden liegen, als habe in unbewusster Form von dem älteren Forscher auf den jüngeren eine Uebertragung leitender Ideen stattgefunden.

matiker im einzelnen so verschieden wie möglich; sie scheinen sich fast zu widerstreiten, was, von einem höherem Standpunkte gesehen, selbstverständlich dahin führt, dass sie einander ergänzen.

Weierstrass definirt die Functionen einer complexen Veränderlichen analytisch durch eine gemeinsame Formel, nämlich die unendlichen Potenzreihen; er vermeidet auch weiterhin nach Möglichkeit geometrische Hülfsmittel und sucht seine specifische Leistung in der durchgebildeten Schärfe der Beweisführung.

Riemann dagegen beginnt — dem allgemeinen Ansatze entsprechend, den ich vorhin bezeichnete, — mit gewissen Differentialgleichungen, denen die Functionen von $x+iy$ genügen. Es nimmt das hier unmittelbar physikalische Form an. Man setze $f(x+iy)=u+iv$. Dann erscheint vermöge der genannten Differentialgleichungen der einzelne Bestandteil, u wie v, als ein Potential in dem Raume der zwei Veränderlichen x und y, und man kann Riemann's Entwickelungen kurzweg dahin bezeichnen, dass er auf diese einzelnen Bestandteile die Grundsätze der Potentialtheorie zur Geltung bringt. Sein Ausgangspunkt liegt hiernach auf dem Gebiete der mathematischen Physik. Sie sehen, dass auch innerhalb der Mathematik der Individualität ein breiter Spielraum bleibt.

Wollen Sie übrigens bemerken, dass die Potentialtheorie, welche nach ihrer Unentbehrlichkeit in der Elektricitätslehre und anderen Capiteln der Physik heutzutage ein allgemein gekanntes und benutztes Instrument ist, damals noch jung war. Allerdings hat Green bereits 1828 seine grundlegende Abhandlung geschrieben, aber diese ist lange unbeachtet geblieben. Dann folgt Gauss 1839. Die Weiterverbreitung und Entwickelung der hier gegebenen Grundsätze ist, soweit Deutschland in Betracht kommt, wesentlich das Verdienst der Vorlesungen von Dirichlet, und an diese knüpft Riemann unmittelbar an.

Als specifische Leistung von Riemann erscheint in diesem Zusammenhange zunächst selbstverständlich die Tendenz, der Potentialtheorie eine grundlegende Bedeutung für die ganze Mathematik zu geben, weiter aber eine Reihe geometrischer Constructionen, oder, wie ich lieber sage, geometrischer Erfindungen, über die Sie mir ein paar Worte gestatten wollen.

Ein erster Schritt ist, dass Riemann die Gleichung $u+iv= f(x+iy)$ durchweg als eine Abbildung der Ebene x, y auf eine Ebene u, v auffasst. Diese Abbildung erweist sich als conform, das heisst winkeltreu, und kann geradezu durch diese Eigenschaft charakterisirt

werden. Wir haben so ein neues Hülfsmittel zur Definition der Functionen von x+iy. Riemann entwickelt in dieser Hinsicht den glänzenden Satz, dass es immer eine Function f giebt, welche ein beliebiges, einfach zusammenhängendes Gebiet der xy-Ebene auf ein beliebig gegebenes, einfach zusammenhängendes Gebiet der uv-Ebene überträgt; diese Function ist bis auf drei Constante, die willkürlich bleiben, völlig bestimmt.

Hierüber hinaus aber begründet er die Vorstellung der Riemann'schen Fläche (wie wir es heute ausdrücken), das heisst einer Fläche, welche sich mehrblättrig über der Ebene ausbreitet, und deren Blätter in sogenannten Windungspunkten zusammenhängen. Dies ist ohne Zweifel der schwierigste, aber auch der erfolgreichste Schritt gewesen. Wir sehen noch täglich, wie hart es dem Neuling ankommt, das Wesen der Riemann'schen Fläche zu begreifen, und wie er auf einmal die ganze Theorie besitzt, wenn er diese fundamentale Vorstellungsweise erfasst hat. Die Riemann'sche Fläche bietet das Mittel, um die mehrwertigen Functionen von x+iy in ihrem Verlaufe zu verstehen. Denn auf ihr existiren ebensolche Potentiale, wie auf der schlichten Ebene, deren Gesetzmässigkeiten mit denselben Mitteln erforscht werden können; nicht minder bleibt die Methode der conformen Abbildung hier in Geltung. Einen ersten Haupteinteilungsgrund giebt dabei die Zusammenhangszahl der Flächen, das heisst die Zahl der Querschnitte, die man ausführen kann, ohne die Fläche in getrennte Teile zu zerlegen. Auch dies ist eine geometrisch ganz neue Fragestellung, die vor Riemann trotz ihres elementaren Charakters von niemand berührt worden war.

Vielleicht bin ich mit diesen Ausführungen bereits zu sehr ins einzelne gegangen. Um so lieber will ich gleich hinzufügen, dass alle diese Hülfsmittel, welche Riemann von der physikalischen Anschauung aus für die Zwecke der reinen Mathematik geschaffen hat, rückwärts für die mathematische Physik die grösste Bedeutung gewonnen haben. Ueberall zum Beispiel, wo es sich um stationäre Strömungen von Flüssigkeiten in Gebieten von zwei Dimensionen handelt, kommen die Riemann'schen Ansätze jetzt allgemein zur Verwendung. Hierdurch ist eine Reihe der interessantesten Aufgaben, die früher unlösbar schienen, erledigt worden. Sehr bekannt ist in dieser Hinsicht Helmholtz's Bestimmung der Gestalt eines freien Flüssigkeitsstrahls. Vielleicht weniger beachtet ist eine andere Art der physikalischen Anwendung, bei welcher die Riemann'schen Vorstellungsweisen in besonders reizvoller Combination zur Geltung kommen. Ich meine die Theorie der Minimal-

flächen. Riemann's eigene Untersuchungen hierüber sind erst 1867 nach seinem Tode publicirt worden, ziemlich gleichzeitig mit parallellaufenden Untersuchungen von Weierstrass über denselben Gegenstand. Seitdem ist die Fragestellung durch Schwarz und andere sehr viel weiter verfolgt worden. Es handelt sich darum, die Gestalt der kleinsten Fläche zu bestimmen, die in einen festen Rahmen eingespannt werden kann, — sagen wir die Gleichgewichtsfigur einer Flüssigkeitslamelle, die in eine gegebene Contour passt. Da ist das Merkwürdige, dass auf Grund der Riemann'schen Ansätze die in der Analysis bekannten Functionen gerade ausreichen, um die einfachsten Fälle zu erledigen.

Diese Anwendungen, die ich heute voranstelle, sind selbstverständlich nur die eine Seite der Sache. Die Hauptbedeutung der functionentheoretischen Methoden, um die es sich handelt, liegt zweifellos nach Seiten der reinen Mathematik. Ich muss versuchen, dies genauer zu entwickeln, wie es der Wichtigkeit des Gegenstandes entspricht, ohne doch dabei besondere Vorkenntnisse vorauszusetzen.

Lassen sie mich mit der ganz allgemeinen Frage beginnen, wie es überhaupt mit dem Fortschritt im Gebiete der reinen Mathematik bestellt ist. Die Weiterbildung der reinen Mathematik erscheint dem Fernerstehenden vielleicht als etwas ganz Willkürliches, weil die Concentration auf einen von Haus aus gegebenen bestimmten Gegenstand wegfällt. Und dennoch giebt es einen Regulator, der in beschränkterem Sinne innerhalb aller anderen Disciplinen wohlbekannt ist — die historische Continuität: Die reine Mathematik wächst, indem man alte Probleme mit neuen Methoden durchdenkt. In dem Maasse, wie wir die früheren Aufgaben besser verstehen, bieten sich neue von selbst.

Von dieser Auffassung geleitet, müssen wir zunächst einen Blick auf das functionentheoretische Material werfen, welches Riemann zu Beginn seiner Laufbahn entgegentrat. Man hatte gefunden, dass unter den analytischen Functionen einer Variablen, das heisst eben unter den Functionen von $x+iy$, drei Klassen der Beachtung ganz besonders wert sind. Es sind dies zunächst die algebraischen Functionen, die durch eine endliche Zahl von Elementaroperationen, das heisst von Additionen, Multiplicationen und Divisionen definirt werden — im Gegensatze zu den transcendenten Functionen, bei deren Festlegung unendliche Reihen der genannten Operationen benötigt werden. Unter den transcendenten Functionen stehen natürlich die Logarithmen und andererseits die trigonometrichen Functionen, also Sinus und Cosinus etc., als die einfachsten

voran. Aber die Forschung war über diese bereits fortgeschritten, einerseits zu den elliptischen Functionen, die aus der Umkehr der elliptischen Integrale erwachsen, dann zu den anderen Functionen, welche mit der Gauss'schen hypergeometrischen Reihe zusammenhängen, den Kugelfunctionen, Bessel'schen Functionen, Gammafunctionen etc.

Die Riemann'sche Leistung kann nun am kürzesten dahin bezeichnet werden, dass er für eine jede dieser drei Functionsklassen ganz neue Resultate und neue Auffassungen gefunden hat, welche bis heute fortschreitend die Quelle nachhaltigster Anregung geblieben sind. Einige wenige Bemerkungen mögen dies mehr im einzelnen vorführen.

Das Studium der algebraischen Functionen fällt dem Wesen nach zusammen mit dem Studium der algebraischen Curven, deren Eigenschaften die Geometer studiren, mögen sie sich zu den „Analytikern" zählen, welche die Formel voranstellen, oder zu den „synthetischen Geometern" im Sinne Steiner's und v. Staudt's, die mit der Erzeugung der Curven durch Strahlbüschel operiren. Der wesentliche neue Gesichtspunkt, den Riemann hier eingeführt hat, ist der Gesichtspunkt der allgemeinen eindeutigen Transformation. Von hier aus erscheinen die vielgestaltigen algebraischen Curven in grosse Kategorien zusammengefasst, und es entsteht, indem man von den Eigentümlichkeiten der einzelnen Curvenform absieht, eine Lehre von den allgemeinen Eigenschaften, die allen zusammengehörigen Curven gemeinsam sind. Die Geometer haben nicht gezögert, die solcherweise entspringenden Resultate von ihrem Standpunkte aus abzuleiten und weiter zu verfolgen, — allen voran Clebsch, der gleich auch begann, die entsprechenden Untersuchungen bei mehrdimensionalen algebraischen Gebilden in Angriff zu nehmen. Aber es wird darauf ankommen, dass die Curvengeometrie auch die Methoden Riemann's nach ihrem inneren Gehalte zu assimiliren sucht. Ein erster Schritt dazu ist, dass man an der Curve selbst das Gegenbild für die zweifach ausgedehnte Riemann'sche Fläche construirt, was in mannigfacher Weise gelingt. Der weitere Fortschritt müsste sein, dass man auf dem so definirten Gebilde functionentheoretisch operiren lernt.

Die Theorie der elliptischen Integrale findet ihre Weiterbildung in der Betrachtung der allgemeinen Integrale algebraischer Functionen, über welche der Norwege Abel in den zwanziger Jahren dieses Jahrhunderts die ersten grundlegenden Untersuchungen publicirt hat. Man wird es immer als eine der grössten Leistungen Jacobi's ansehen müssen, dass er durch eine Art von Divination für diese Integrale ein Umkehrproblem aufstellte, welches, ebenso wie im Falle der elliptischen Integrale

die directe Umkehr, eindeutige Functionen ergiebt. Die wirkliche Durchführung dieses Umkehrproblems ist die centrale Aufgabe, welche auf verschiedenen Wegen gleichzeitig von Weierstrass und Riemann gelöst worden ist. Man hat die grosse Abhandlung über die Abel'schen Functionen, in welcher Riemann 1857 seine Theorie veröffentlichte, unter allen Leistungen seines Genius immer als die glänzendste betrachtet. Denn das Resultat kommt nicht auf mühsamem Wege, sondern durch unmittelbare Betrachtungen hervor, einfach indem Riemann in geeigneter Ideenverbindung die geometrischen Hülfsmittel heranzieht, von denen soeben andeutungsweise die Rede war. Ich habe bei einer früheren Gelegenheit gezeigt, dass man seine Resultate, betreffend die Integrale, sowie die daraus folgenden Ergebnisse, betreffend die algebraischen Functionen, in übersichtlichster Weise erhält, indem man stationäre Flüssigkeitsströmungen, sagen wir Strömungen der Elektricität, auf beliebig im Raume gelegenen geschlossenen Flächen betrachtet. Doch betrifft das nur die erste Hälfte der Riemann'schen Abhandlung. Die zweite Hälfte, welche sich auf die Thetareihen bezieht, ist vielleicht noch bemerkenswerter. Es ergiebt sich da das merkwürdige Resultat, dass die Thetareihen, deren man zur Erledigung des Jacobi'schen Umkehrproblems bedarf, nicht die allgemeinen sind, womit die neue Aufgabe gegeben ist, die Stellung der allgemeinen Theta in dieser Theorie zu bestimmen. Nach einer Notiz von Hermite hat Riemann bereits den Satz gekannt, der später von Weierstrass publicirt und neuerdings von Picard und Poincaré behandelt wurde, nämlich dass die Thetareihen ausreichen, um die allgemeinsten periodischen Functionen mehrerer Variablen aufzustellen.

Doch ich darf auf diese Einzelfragen nicht zu weit eingehen. Eine zusammenhängende Darstellung der Entwickelung zu geben, welche an Riemann's Abel'sche Functionen anschliesst, ist darum misslich, weil die weitgehenden Untersuchungen von Weierstrass über denselben Gegenstand immer nur erst aus Vorlesungsheften bekannt sind. Ich werde mich also auf die Bemerkung beschränken, dass das wichtige Buch von Clebsch und Gordan, das 1866 erschien, im wesentlichen bezweckte, die Riemann'schen Resultate an der algebraischen Curve mit den Hülfsmitteln der analytischen Geometrie zur Ableitung zu bringen. Die Riemann'schen Methoden waren damals noch eine Art Arcanum seiner directen Schüler und wurden von den übrigen Mathematikern fast mit Misstrauen betrachtet. Ich kann dem gegenüber nur wiederholen, was ich soeben bei den Curven bemerkte, dass nämlich die fortschreitende

Entwickelung ersichtlich mit Notwendigkeit dahin führt, auch die Riemann'schen Methoden dem Allgemeinbesitz der Mathematiker einzufügen. Es ist interessant, in dieser Hinsicht die neusten französischen Lehrbücher zu vergleichen*).

Die dritte Functionsklasse, die wir nannten, sollte diejenigen Abhängigkeitsgesetze umfassen, welche sich an die Gauss'sche hypergeometrische Reihe anschliessen. Es sind dies im weiteren Sinne diejenigen Functionen, die durch lineare Differentialgleichungen mit algebraischen Coefficienten definirt werden können. Riemann hat hierüber bei seinen Lebzeiten nur eine erste einleitende Arbeit veröffentlicht (1856), welche sich ausschliesslich mit dem hypergeometrischen Falle selbst beschäftigt und in überraschender Weise zeigt, wie alle die früher bekannten merkwürdigen Eigenschaften der hypergeometrischen Function ohne alle Rechnung aus dem Verhalten der Function bei Umkreisung der singulären Punkte abgeleitet werden können. Wir wissen jetzt aus seinem Nachlasse, in welcher Form er sich die entsprechende allgemeine Theorie der linearen Differentialgleichungen $n$ter Ordnung ausgeführt dachte: auch hier sollte die Gruppe der linearen Substitutionen, welche die Lösungen bei Umkreisung der singulären Punkte erleiden, voranstehen und das oberste Merkmal der Klassification abgeben.

Dieser Ansatz, welcher gewissermaassen der von Riemann gegebenen Behandlung der Abel'schen Integrale entspricht, ist in der umfassenden von Riemann beabsichtigten Weise noch nicht durchgeführt worden; die zahlreichen Untersuchungen über lineare Differentialgleichungen, welche in den letzten Jahrzehnten anderweitig publicirt worden sind, haben im wesentlichen nur erst einzelne Teile der Theorie geordnet. Es sind in dieser Hinsicht insbesondere die Untersuchungen von Fuchs zu nennen. Uebrigens ist die Theorie, sofern man sich auf lineare Differentialgleichungen der zweiten Ordnung beschränkt, einer einfachen geometrischen Interpretation fähig. Man hat die conforme Abbildung zu betrachten, welche der Quotient zweier Particularlösungen der Differentialgleichung von dem Gebiet der unabhängigen Veränderlichen entwirft. Im einfachsten Falle der hypergeometrischen Function erhält man hier die Abbildung einer Halbebene auf ein Kreisbogendreieck und damit einen merkwürdigen Uebergang zur sphärischen Trigonometrie. Allgemein giebt es Fälle, welche eindeutige Umkehr gestatten und damit zu jenen be-

*) Vergleiche Picard, Traité d'analyse, Appel et Goursat, Théorie des fonctions algébriques et de leurs intégrales.

merkenswerten Functionen einer Variablen Anlass geben, die gleich den periodischen Functionen durch unendlich viele lineare Transformationen in sich übergehen, und die ich dem entsprechend als automorphe Functionen bezeichne. Alle diese Entwickelungen, welche die Functionentheoretiker der Neuzeit beschäftigen, treten mehr oder minder explicite bereits in den hinterlassenen Papieren Riemann's auf, insbesondere in der Arbeit über die Minimalflächen, von welcher oben die Rede war. Ich verweise übrigens auf Schwarz' Abhandlung über die hypergeometrische Reihe und auf die bahnbrechenden Untersuchungen von Poincaré zur Theorie der automorphen Functionen. Hier rubriciren auch die Untersuchungen über die elliptischen Modulfunctionen und die Functionen der regulären Körper.

Ich darf die Besprechung von Riemann's functionentheoretischen Arbeiten nicht schliessen, ohne einer isolirt stehenden Abhandlung zu gedenken, in welcher derselbe interessante Beiträge zur Theorie der bestimmten Integrale giebt, die aber zumal durch die Anwendung, welche Riemann auf ein zahlentheoretisches Problem macht, berühmt geworden ist. Es handelt sich um das Gesetz der Verteilung der Primzahlen innerhalb der natürlichen Zahlenreihe. Riemann giebt für dasselbe Annäherungsausdrücke, welche sich wesentlich näher an die Ergebnisse der empirischen Abzählungen anschliessen, als die bis dahin aus diesen Abzählungen inductiv abgeleiteten Regeln. Zwei Bemerkungen sind es, die sich hier aufdrängen. Erstlich wollen Sie beachten, wie merkwürdig die einzelnen Teile der höheren Mathematik zusammenhängen, indem hier ein Problem, welches in die Elemente der Zahlenlehre zu gehören scheint, aus den Entwickelungen der feinsten functionentheoretischen Fragen eine ungeahnte Förderung erfährt. Zweitens aber habe ich hervorzuheben, dass die Beweise der Riemann'schen Abhandlung, wie er übrigens selbst bemerkt, nicht ganz vollständig sind, und dass dieselben trotz zahlreicher Bemühungen der neusten Zeit noch nicht lückenlos haben hergestellt werden können. Riemann muss vielfach mit der Intuition gearbeitet haben. Es gilt dies auch, wie ich nicht verfehlen darf, nachträglich anzugeben, für seine Grundlegung der Functionentheorie selbst. Riemann verwendet dort eine in der mathematischen Physik oft gebrauchte Schlussweise, die er seinem Lehrer Dirichlet zu Ehren als Dirichlet'sches Princip bezeichnet. Es handelt sich darum, eine stetige Function zu bestimmen, welche ein gewisses Doppelintegral zu einem Minimum macht, und hier behauptet nun das genannte Princip, dass die Existenz einer solchen Function aus der Fragestellung selbst

evident sei*). Weierstrass hat gezeigt, dass hier ein Fehlschluss vorliegt; es könnte sein, dass das Minimum, welches wir suchen, nur eine Grenze bezeichnet, welche man innerhalb des Gebietes der stetigen Functionen nicht erreichen kann. Hiermit wird ein grosser Teil der Riemannschen Entwickelungen hinfällig. Trotzdem aber sind die weitreichenden Resultate, welche Riemann auf das genannte Princip stützt, alle richtig, wie dies Carl Neumann und Schwarz durch strenge Methoden später ausführlich gezeigt haben. Man muss sich wohl die Idee bilden, dass Riemann die Theoreme selbst ursprünglich der physikalischen Anschauung entnommen hat, die sich hier wieder einmal als heuristisches Princip bewährte, und nur hinterher auf die genannte Schlussweise bezog, um einen in sich geschlossenen mathematischen Gedankengang zu haben. Hierbei hat er, wie längere Entwickelungen seiner Dissertation zeigen, gewisse Schwierigkeiten sehr wohl gefühlt, aber im Hinblicke darauf, dass er die Schlussweise in analogen Fällen von seiner Umgebung, selbst von Gauss, anstandslos angenommen sah, nicht so weit verfolgt, als erforderlich gewesen wäre.

So viel über die Functionen complexer Variabler. Sie repräsentiren das einzige Gebiet, welches Riemann im Zusammenhange bearbeitet hat; alles andere sind Einzeluntersuchungen. Aber man würde doch ein sehr unzureichendes Bild von dem Mathematiker Riemann erhalten, wenn man darum diese anderen Arbeiten zur Seite schieben wollte. Denn abgesehen von den sehr bemerkenswerten Resultaten, welche er in denselben gewinnt, lassen sie erst die allgemeine Auffassung hervortreten, die ihn beherrschte, und das Arbeitsprogramm, welches er auszuführen dachte. Auch hat eine jede dieser Untersuchungen in hervorragendem Maasse anregend und bestimmend auf die Weiterentwickelung der Wissenschaft eingewirkt, wie ich sofort des näheren ausführen werde.

Sagen wir es vor allen Dingen, was wir schon oben andeuteten, dass die von Riemann gegebene Behandlung der Functionentheorie complexer Variabler, welche von der partiellen Differentialgleichung des Potentials beginnt, nach seiner Auffassung nur ein Beispiel für eine

*) Ich verstehe hier also unter dem „Princip" entgegen einem vielfach verbreiteten Sprachgebrauche die Schlussweise, nicht die daraus abgeleiteten Resultate. Bei der Gelegenheit möchte ich auf einen Aufsatz von W. Thomson aufmerksam machen, der in Liouville's Journal, Bd. XII, 1847 abgedruckt ist und von den deutschen Mathematikern zu wenig beachtet zu sein scheint. Das fragliche Princip ist dort in grosser Allgemeinheit ausgesprochen.

analoge Behandlung aller anderen physikalischen Probleme sein sollte, die auf partielle Differentialgleichungen — oder überhaupt auf Differentialgleichungen — führen; allemal soll gefragt werden, welches die mit den Differentialgleichungen verträglichen Unstetigkeiten sind, und wie weit die Lösungen durch die bei ihnen hervortretenden Unstetigkeiten und zutretende Nebenbedingungen bestimmt sein mögen. Die Durchführung dieses Programms, welches seitdem von verschiedenen Seiten wesentlich gefördert ist und in den letzten Jahren mit besonderem Erfolge von den französischen Geometern aufgenommen wurde, kommt auf nichts Geringeres als eine systematische Neubegründung der Integrationsmethoden der Mechanik und mathematischen Physik hinaus. Riemann hat selbst in dieser Hinsicht nur ein einzelnes Problem eingehender behandelt. Es geschieht dies in der Abhandlung über die Fortpflanzung ebener Luftwellen von endlicher Schwingungsweite, 1860. Man muss bei den linearen partiellen Differentialgleichungen der mathematischen Physik zwei Haupttypen unterscheiden: den elliptischen und den hyperbolischen Typus, für welche beziehungsweise die Differentialgleichung des Potentials und die Differentialgleichung der schwingenden Saite die einfachsten Beispiele bilden; ihnen tritt als ein Uebergangsfall der parabolische Typus zur Seite, unter den die Differentialgleichung der Wärmeleitung rubricirt. Neuere Untersuchungen von Picard haben gezeigt, dass man die Integrationsmethoden der Potentialtheorie ziemlich ungeändert auf die elliptischen Differentialgleichungen überhaupt übertragen kann. Aber wie ist es bei den anderen Typen? In dieser Hinsicht giebt Riemann's Arbeit einen ersten wichtigen Beitrag. Riemann zeigt, welche merkwürdigen Modificationen an der aus der Potentialtheorie bekannten Randwertaufgabe und ihrer Lösung durch die Green'sche Function angebracht werden müssen, damit die Entwickelung für die hyperbolischen Differentialgleichungen gültig bleibe. Aber auch nach anderer Seite ist die Riemann'sche Abhandlung besonders bemerkenswert. Schon die Reduction des in der Ueberschrift genannten Problems auf eine lineare Differentialgleichung ist eine besondere Leistung. Und daneben zieht sich durch die Abhandlung eine Betrachtungsweise, die dem Physiker allerdings kaum überraschend sein wird: die graphische Behandlung des Problems. Ich möchte hierauf ganz besonders aufmerksam machen. Denn die in Rede stehende Methode wird seitens der an abstractere Ueberlegungen gewöhnten Mathematiker heutzutage vielfach unterschätzt. Um so erfreulicher ist es, dass eine mathematische Auto-

rität wie Riemann deren Gebrauch an geeigneter Stelle vertritt und aus ihr die merkwürdigsten Folgerungen zu ziehen weiss.

Es bleiben nun noch die beiden grossen Entwürfe zu besprechen, welche Riemann 1854, im Alter von 28 Jahren, bei seiner Habilitation vorgelegt hat: der Aufsatz über die Hypothesen, welche der Geometrie zu Grunde liegen, und die Schrift über die Darstellbarkeit einer Function durch eine trigonometrische Reihe. Es ist merkwürdig, wie verschieden diese beiden Arbeiten bisher von dem allgemeineren wissenschaftlichen Publicum gewertet worden sind: Die Hypothesen der Geometrie haben seit lange die ihnen gebührende allgemeine Beachtung gefunden, hauptsächlich jedenfalls durch das Eintreten von Helmholtz, wie viele von Ihnen wissen; die Untersuchung über die trigonometrische Reihe aber ist bislang nur im engeren Kreise der Mathematiker bekannt. Dies hindert nicht, dass die Resultate, welche sie enthält, oder, ich will lieber sagen, die Betrachtungen, zu denen sie Anlass gegeben hat, oder mit denen sie im Zusammenhange steht, vom allgemeinen erkenntnistheoretischen Standpunkte aus das höchste Interesse beanspruchen.

Was die Hypothesen der Geometrie angeht, so werde ich hier mich nicht weiter über die philosophische Bedeutung der Sache verbreiten, über die ich nichts Neues zu sagen habe. Es handelt sich bei dieser Discussion für den Mathematiker weniger um den Ursprung der geometrischen Axiome, als um deren gegenseitige logische Abhängigkeit. Die berühmteste Frage ist jedenfalls die nach der Stellung des Parallelenaxioms. Die Untersuchungen von Gauss, Lobatschefskij und Bolyai (um nur die hervorragendsten Namen zu nennen) haben bekanntlich gezeigt, dass das Parallelenaxiom gewiss keine Folge der übrigen Axiome ist, dass man eine allgemeine, in sich consequente Geometrie aufbauen kann, welche die gewöhnliche Geometrie als Specialfall enthält, indem man vom Parallelenaxiom absieht. Diesen wichtigen Betrachtungen hat Riemann dadurch eine neue und specifische Wendung gegeben, dass er die Ideenbildungen der analytischen Geometrie voranstellt: der Raum erscheint ihm als ein besonderer Fall einer dreifach ausgedehnten Zahlenmannigfaltigkeit, in welcher sich das Quadrat des Bogenelementes durch eine quadratische Form der Differentiale der Coordinaten ausdrückt. Die speciellen geometrischen Resultate, welche er von hier aus gewinnt, werde ich nicht weiter besprechen und noch weniger auf die Weiterentwickelung eingehen, welche die Theorie in der Zwischenzeit von anderer Seite gefunden hat. Das Wesentliche in dem

vorliegenden Zusammenhange ist, dass Riemann auch hier seinem Grundgedanken treu geblieben ist: die Eigenschaften der Dinge aus ihrem Verhalten im Unendlichkleinen zu verstehen. Er hat dabei den Grund zu einem neuen Capitel der Differentialrechnung gelegt: zur Lehre von den quadratischen Differentialausdrücken beliebiger Variabler, beziehungsweise von den Invarianten, welche diese Differentialausdrücke gegenüber beliebigen Transformationen der Variabeln besitzen. Ich will hier, in Ergänzung der sonstigen Betrachtungen meines Vortrages, einmal diese abstracte Seite der Sache hervorheben. Gewiss ist es bei der Auffindung mathematischer Beziehungen nicht gleichgültig, ob man den Symbolen, mit welchen man operirt, eine bestimmte Bedeutung beilegt oder nicht, indem sich gerade aus der concreten Auffassung diejenigen Gedankenverbindungen ergeben, welche weiterführen. Beleg hierfür ist so ziemlich alles, was wir bisher über die innere Verwandtschaft der Riemann'schen Mathematik und der mathematischen Physik sagten. Aber unabhängig davon steht das schliessliche Resultat der mathematischen Untersuchungen oberhalb aller derartiger specieller Ansätze; es ist ein allgemeines logisches Schema, dessen besonderer Inhalt gleichgültig bleibt und je nachdem in verschiedener Weise gewählt werden kann. Von diesem Standpunkte aus hat es nichts Ueberraschendes, dass Riemann später (1861) in einer der Pariser Akademie eingereichten Preisaufgabe von seiner Untersuchung über die Differentialausdrücke eine Anwendung auf ein Problem der Wärmeleitung macht, also auf einen Gegenstand, der mit den Hypothesen der Geometrie gewiss nichts zu thun hat. In demselben Sinne schliessen sich hier moderne Untersuchungen über die Aequivalenz und Klassification der allgemeinen mechanischen Probleme an. In der That kann man die Differentialgleichungen der Mechanik nach Lagrange und Jacobi in der Weise darstellen, dass sie von einer einzigen quadratischen Form der Differentiale der Coordinaten abhängen.

Ich komme nun zu der Arbeit über die trigonometrische Reihe, die ich mit Vorbedacht an das Ende gesetzt habe, weil sie einen letzten wesentlichen Charakter der Riemann'schen Auffassung hervortreten lässt. Bei meiner bisherigen Darstellung konnte ich allemal kurzweg an die geläufigen Vorstellungsweisen der Physik oder doch der Geometrie anknüpfen. Aber der eindringende Geist Riemann's hat sich nicht damit begnügt, die geometrisch-physikalische Anschauung zu benutzen; er ist dazu übergegangen, dieselbe zu kritisiren und nach der Notwendigkeit der aus ihr fliessenden mathematischen Beziehungen zu

fragen. Es handelt sich, kurz gesagt, um die Principien der Infinitesimalrechnung. Riemann hat in seinen sonstigen Arbeiten zu den in dieser Richtung vorliegenden Problemen immer nur beiläufig oder versteckt Stellung genommen. Anders in der Arbeit über die trigonometrische Reihe. Er behandelt ja da leider nur einzelne Probleme: die Frage, ob eine Function in jedem Punkte unstetig sein könne, und ob bei Functionen von so allgemeiner Beschaffenheit unter Umständen noch von einer Integration möchte gesprochen werden können. Aber diese Probleme behandelt er in so überzeugender Weise, dass von hier aus die Untersuchungen anderer über die Grundlagen der Analysis den mächtigsten Impuls erhalten haben. Die Tradition berichtet, dass Riemann in späteren Jahren seinen Schülern denjenigen Punkt bezeichnete, der als das merkwürdigste Ergebnis der modernen Kritik dasteht: die Existenz stetiger Functionen, die an keiner Stelle differentiirbar sind. Ausführlicheres über derartige „unvernünftige" Functionen (wie man lange sagte) ist dann freilich erst durch Weierstrass bekannt geworden, der überhaupt wohl das Meiste dazu beigetragen hat, um die Theorie reeller Functionen reeller Variabler (wie man das ganze hier vorliegende Gebiet zu nennen pflegt) in seine heutige strenge Gestalt zu bringen. Ich verstehe die Riemann'schen Entwickelungen über die trigonometrische Reihe so, dass er mit der Weierstrass'schen Darlegungsweise, welche in den hier vorliegenden Fragen die räumliche Anschauung verbannt und ausschliesslich mit arithmetischen Definitionen operirt, was die Grundlegung angeht, einverstanden sein würde. Aber ich kann mir nicht denken, dass Riemann darum in seinem Herzen die räumliche Anschauung, wie es jetzt wohl von übereifrigen Vertretern der modernen Richtung geschieht, als etwas der Mathematik Widerstreitendes, welches notwendig zu Fehlschlüssen verleiten müsste, angesehen hat. Er muss daran festgehalten haben, dass in der Schwierigkeit, welche hier vorliegt, ein Ausgleich möglich ist.

Wir berühren hier eine Frage, welche für die Weiterentwickelung der Mathematik gerade in der Gegenwart von entscheidender Wichtigkeit sein dürfte: Unsere Studirenden wachsen zur Zeit heran, indem sie gleich anfangs alle die intricaten Verhältnisse kennen lernen, welche die moderne Analysis als möglich aufgedeckt hat. Das ist gewiss gut, aber es hat eine bedenkliche Folgeerscheinung, dass nämlich die jungen Mathematiker sich vielfach scheuen, überhaupt bestimmte Sätze zu formuliren, dass ihnen die Frische fehlt, ohne welche auch in der Wissenschaft kein Erfolg errungen werden kann. Auf der anderen Seite glaubt die Mehr-

zahl der Praktiker sich den angedeuteten schwierigen Untersuchungen einfach entziehen zu dürfen. Sie lösen sich dadurch von der strengen Wissenschaft ab und entwickeln für ihren Hausgebrauch eine besondere Mathematik, die wie ein Wurzelschössling neben der veredelten Pflanze emporschiesst. Wir werden alles einsetzen wollen, dass die hier vorliegende gefährliche Spaltung überwunden wird. Sei es dem entsprechend gestattet, mit zwei Sätzen meine eigene Stellung in dieser Sache zu präcisiren:

Erstlich glaube ich, dass die von mathematischer Seite gerügten Mängel der räumlichen Anschauung nur temporäre sind, dass man die Anschauung üben kann, so dass man mit ihrer Hülfe die abstracten Entwickelungen der Analytiker jedenfalls in ihrer Tendenz versteht.

Ich glaube ferner, dass bei der so geforderten Ausbildung der Anschauuung die Anwendungen der Mathematik auf Gegenstände der Aussenwelt in der Hauptsache ungeändert bestehen bleiben, sofern man sich nur entschliesst, dieselben durchweg als eine Art von Interpolation gelten zu lassen, welche die Verhältnisse mit einer den praktischen Anforderungen genügenden, aber doch nur begrenzten Genauigkeit darstellt.

Mit diesen Bemerkungen darf ich meinen Vortrag, der Ihre Geduld schon zu lange in Anspruch genommen hat, schliessen. Sie mögen erkannt haben, dass auch innerhalb der Mathematik kein Stillstand ist, dass eine ähnliche Bewegung herrscht, wie in den Naturwissenschaften. Und auch dieses ist ein allgemeines Gesetz, dass zwar viele zur Entwickelung der Wissenschaft beitragen, dass aber die wirklich neuen Anregungen nur auf wenige hervorragende Forscher zurückgehen. Deren Wirksamkeit ist dann nicht auf die kurze Spanne ihres Lebens beschränkt; sie wirken nach, indem sie allmählich in immer vollerem Maasse verstanden werden. So ist es zweifellos mit Riemann. Ich möchte, dass Sie meine heutigen Ausführungen nicht als die Schilderung einer zurückliegenden Zeit ansehen, der wir die Empfindungen der Pietät widmen, sondern als eine Wiedergabe lebendiger Momente, welche die Mathematik der Gegenwart erfüllen.

Lobatschefskij's Ansichten über die Theorie der Parallellinien vor dem Jahre 1826.

Von

A. Wassiljef (Kasan).

Die Frage, wie Lobatschefskij auf seine eigentümlichen Ansichten über die Theorie der Parallellinien gekommen ist, die zum ersten Male, aber in einer ausgearbeiteten Form, im Jahre 1826 in der Sitzung der Physico-mathematischen Abteilung der Universität Kasan auseinandergesetzt wurden, wird vielleicht für immer unentschieden bleiben; es bleibt also ungewiss, ob er in irgend welcher Weise seinem Lehrer Bartels, Gauss' Freunde, für eine Anregung, sich mit dieser Theorie zu beschäftigen, verpflichtet ist. In den von ihm hinterlassenen Manuscripten, die sich auf eine viel spätere Zeit beziehen, kann man darüber keine Angaben finden. Es war auch nicht möglich, eine Copie eines Lehrbuches der Geometrie, das von Lobatschefskij im Jahre 1823 für die Gymnasien geschrieben wurde und von dem Akademiker Fuss einer schroffen Kritik unterzogen worden war*), aufzufinden. Deshalb war ich sehr erfreut, als man mir ein altes Heft brachte, das die Vorlesungen, welche Lobatschefskij in den Jahren 1815—1816 an der Universität gehalten hatte, enthält. In diesen Vorlesungen finden sich drei Abrisse einer systematischen Bearbeitung der elementaren Geometrie, und in jedem von diesen Abrissen finden sich drei ganz verschiedene Auffassungen der Parallelentheorie.

Dem Beispiele von L. A. Sohncke in Ersch's und Gruber's „Allgemeine Encyclopädie der Wissenschaften und Künste" folgend, kann man alle Versuche, welche zur Vervollständigung der Parallelentheorie gemacht sind, in drei Klassen teilen. In die erste Klasse kommen die Versuche, in welchen eine neue, von der Euklidischen abweichende Definition der Parallellinien zu Grunde gelegt wird. Man definirt die Parallellinien als solche, welche in allen Punkten gleich weit von einander abstehen, oder als solche, welche eine und dieselbe Richtung haben. Dieser letzteren Meinung schliesst sich Lobatschefskij in seinem ersten Vorlesungshefte an. Diese Auffassung der Parallelentheorie, auf den Begriff der Richtung

*) Ueber diese Kritik siehe Nikolaj Jwanowitsch Lobachefskij. Rede, gehalten bei der feierlichen Versammlung der Kaiserlichen Universität Kasan am 22. October 1893 von Prof. A. Wassiljef. Aus dem Russischen übersetzt von Prof. Friedrich Engel. (Abhandlungen zur Geschichte der Mathematik, Heft VII, S. 220. Leipzig 1895.)

gestützt, war besonders vollständig von Jacobi in seinem Werke „De undecimo Euclidis axiomate judicium — Jena, 1824" entwickelt, aber vor dem Jahre 1815 findet man sie nur in einem holländischen Werke von van Swinden: „Grondbeginsels der Meetkunde — Amsterdam, 1790".

Es giebt eine andere Klasse von Beweisen, bei welchen man Unendlichkeitsbetrachtungen einführt und mit unendlich grossen Teilen der Ebene operirt. Diese Art Beweise, von Bertrand de Genève in seinem Buche: „Développement nouveau de la partie élémentaire des mathématiques, 1778" zuerst eingeführt, ist vielfach auch von Legendre benutzt worden. Der ähnliche Beweis, den Lobatschefskij in dem zweiten Vorlesungshefte giebt, ist am meisten dem Beweise ähnlich, welchen Crelle in dem Aufsatze: „Ueber die Parallelentheorien und das System in der Geometrie, Berlin, 1816" gegeben hat; später hat ihn Crelle in der Abhandlung: „Theorie der Parallelen", Crelle's Journal Bd. XI, abgedruckt.

Am interessantesten aber ist das dritte Heft; dieses enthält den Beweis des Satzes, dass die Summe der Winkel in einem Dreiecke gleich zwei Rechten ist. Der Beweis schliesst sich am nächsten den Legendre'schen Beweisen an und zeigt eine eingehende Beschäftigung mit den Arbeiten Legendre's über diesen Gegenstand. Vor allem beweist Lobatschefskij, dass die Summe der Winkel zwei Rechte nicht übersteigen kann; dann beweist er, dass, wenn in einem Dreiecke die Summe gleich zwei Rechten ist, es auch ebenso in allen Dreiecken ist. Dann braucht man also nur ein Dreieck zu finden, in welchem die Summe gleich zwei Rechten ist; Lobatschefskij glaubt beweisen zu können, dass in einem rechtwinkligen Dreiecke, in welchem ein spitzer Winkel gleich $\frac{\pi}{8}$ ist, die Summe der Winkel zwei Rechten gleich ist. Gegen den Beweis von Lobatschefskij kann man dieselben Einwände machen wie gegen die Beweise von Legendre. In historischer Beziehung sind seine Theoreme dadurch interessant, dass hier schon bei ihm verschiedene Theoreme über Defecte vorkommen. Er benutzt z. B. bei seinem Beweise das Theorem, dass die Summe der Winkel eines Dreiecks, das in einem anderen enthalten ist, aber mit ihm einen Winkel und eine Seite gemeinschaftlich hat, grösser als die Summe der Winkel des grösseren sein muss. Solche Theoreme gehören schon dem Gebiete der nicht-euklidischen Geometrie an.

Man sieht also, dass Lobatschefskij von den verschiedensten Seiten die Parallelentheorie aufgefasst hatte, dass er zu den verschiedensten Hülfsmitteln griff, um sie zu vervollständigen. Wir können also ver-

sichert sein, dass es mindestens eine zehnjährige Gedankenarbeit war, die zu der Schöpfung der nicht-euklidischen Geometrie führte. Es finden also auch in dem Beispiele der nicht-euklidischen Geometrie die schönen Worte des grossen Newton Bestätigung, dass man zu den grossen Schöpfungen nur durch eine beständige, continuirliche Denkthätigkeit kommt.

Zur Theorie der Differentialgleichungen.

Von

L. Königsberger (Heidelberg).

Der Vortrag stellt sich die Aufgabe, nachdem die Existenz und die Eigenschaften irreducibler gewöhnlicher und partieller Differentialgleichungen erkannt worden, das Analogon zu dem bekannten Satze aufzufinden, dass, wenn ein Zweig einer irreduciblen algebraischen Function einer gewöhnlichen oder partiellen Differentialgleichung Genüge leistet, auch alle anderen Zweige Integrale dieser Differentialgleichung sind. Der für Differentialgleichungen aller Ordnungen sich ergebende Satz mag an dieser Stelle nur für eine gewöhnliche irreducible Differentialgleichung m-ter Ordnung

$$(1.) \qquad f\left(x_1, x_2, y, \frac{dy}{dx_2}, \cdots, \frac{d^m y}{dx_2^m}\right) = 0$$

und eine partielle Differentialgleichung zweiter Ordnung

$$(2.) \qquad \frac{\partial^2 y}{\partial x_1^2} = F\left(x_1, x_2, y, \frac{\partial y}{\partial x_1}, \frac{\partial y}{\partial x_2}, \frac{\partial^2 y}{\partial x_1 \partial x_2}, \frac{\partial^2 y}{\partial x_2^2}\right),$$

welche ein gemeinsames Integral y_1 haben sollen, ausgesprochen werden:

Wenn man die Differentialgleichung (1.) zweimal nach x_1 differentiirt und überall $\frac{\partial^2 y}{\partial x_1^2}$ durch die rechte Seite der Gleichung (2.) ersetzt, so wird die so entstehende Differentialgleichung durch jedes Integral der Differentialgleichung (1.) befriedigt, wenn y_1 nicht schon das Integral einer partiellen Differentialgleichung ist, deren Ordnung in Bezug auf x_1 die erste, in Bezug auf x_2 die $(m-1)$te ist. Auch ohne die letztere Annahme gilt ein ganz allgemeiner Satz, dessen Ausführung hier zu weit führen würde.*)

*) Vergl. Journal für Mathematik, Bd. CXV, S. 23—32.

Ueber die zu einem algebraischen Gebilde gehörigen, auf dem Gebilde nirgends singulären linearen Differentialgleichungen der zweiten Ordnung.

Von

F. Klein (Göttingen).

Die homogene Bezeichnungsweise giebt das Mittel, um die in der Ueberschrift genannten Differentialgleichungen, deren es bekanntlich ∞^{3p-3} giebt, in einfacher Form hinzuschreiben. Man denke sich das Gebilde als kanonische Riemann'sche Fläche gegeben und setze die zugehörige complexe Variable $x = x_1 : x_2$ (vergl. meinen Aufsatz über Abel'sche Functionen in Band 36 der mathematischen Annalen, 1889). Eine derartige Fläche hat die Eigentümlichkeit, dass ihre Windungspunkte die Nullpunkte einer zur Fläche gehörigen algebraischen ganzen Form, der Verzweigungsform σ, sind. Dieses bedingt, dass die Blätterzahl m der Fläche ein Teiler von $2p-2$ ist. Ich setze $2p-2 = m\delta$ und habe dann als Grad der Verzweigungsform $\delta+2$. Nun sei ferner Ω die allgemeinste auf der Fläche existirende ganze algebraische Form vom Grade 2δ; Σ bezeichne eine Form vom Grade $3\delta+2$, die so bestimmt werden muss, dass der Quotient $\frac{\Sigma}{\sigma}$ in den Verzweigungspunkten in bestimmter Weise unendlich wird. Ich bezeichne endlich mit Π die unbekannte Form, welche durch die Differentialgleichung definirt werden soll, und wähle ihren Grad $= -\frac{\delta}{2}$. Die aufzustellende Differentialgleichung lautet dann einfach:

$$(\Pi, \sigma^2)_2 = \left(\frac{\Sigma}{\sigma} + \Omega\right)\Pi.$$

Hier steht linker Hand die zweite Ueberschiebung von Π über das Quadrat der Verzweigungsform σ*).

Als Beispiel nehme man eine ebene Curve vierter Ordnung vom Geschlechte 3, die in gewöhnlicher Weise durch die Gleichung

$$f(x_1, x_2, x_3) = 0$$

gegeben sein soll. Wir erhalten eine kanonische Darstellung, sobald wir hier x_3 als Function von x_1 und x_2 auffassen. Die zugehörige Ver-

---

*) Ich hatte ursprünglich den Term mit Σ fortgelassen; auf die Notwendigkeit desselben hat mich Herr Pick aufmerksam gemacht.

zweigungsform σ ist durch die Polare

$$\frac{\partial f}{\partial x_3} = f_3$$

vorgestellt. Andererseits coincidirt das Ω mit der allgemeinsten ternären quadratischen Form:

$$\sum_1^3 a_{i\varkappa} x_i x_\varkappa$$

(welche ja in der That $3p-3$, d. h. 6 Constante enthält). Endlich kann für Σ der Ausdruck

$$\frac{1}{6}\frac{\partial H}{\partial x_3} = \frac{1}{6} H_3$$

genommen werden, unter H die Hesse'sche von f verstanden. Die Differentialgleichung wird also

$$(\Pi, f_3^2)_2 = \left(\frac{1}{6}\frac{H_3}{f_3} + \Sigma a_{i\varkappa} x_i x_\varkappa\right)\Pi.$$

Hier ist Π vom Grade $-\frac{1}{2}$ zu nehmen und die Ueberschiebung natürlich so aufzufassen, dass x_3 dabei als Function von x_1 und x_2 gilt; d. h. es ist

$$\frac{d}{dx_1} = \frac{\partial}{\partial x_1} + \frac{\partial}{\partial x_3} \cdot \frac{dx_3}{dx_1}$$

zu nehmen u. s. w.

Das Zerfallen von Curven in gerade Linien.

Von

P. Gordan (Erlangen).

(Die Arbeit ist im 45. Bande der mathematischen Annalen, S. 410—427, veröffentlicht.)

Die Resultantenbildungen der Trigonometrie.

Von

Franz Meyer (Clausthal).

In der neueren Algebra wird die Resultante eines Systems von Formen nicht mehr als linke Seite der Eliminationsgleichung betrachtet, sondern als eine selbständige Bildung, als eine gewisse lineare Combination der gegebenen Formen.

Diese Auffassung der Resultante lässt sich auch mit Vorteil in der elementaren Trigonometrie, in der ja fortwährend von Eliminationsprocessen Gebrauch gemacht wird, zum Ausdruck bringen. Der Erfolg ist wesentlich der, dass die verschiedenartigen Formeln sich zu einem organischen Ganzen zusammenschliessen, so dass man von jedem Formelsystem mit verhältnismässiger Leichtigkeit zu jedem anderen übergehen kann.

Um das durch einige Beispiele zu erläutern, gehen wir etwa von dem Cosinus-Satze der sphärischen Trigonometrie aus:

$$\cos a = \cos b \cos c + \sin b \sin c \cos \alpha,$$

aus dem man nach Lagrange alle übrigen Formeln durch Eliminationsprocesse ableiten kann.

An Stelle von a, b, c, α, β, γ schreiben wir lieber a_1, a_2, a_3, α_1, α_2, α_3, verstehen aber jetzt darunter sechs unbeschränkt veränderliche Argumente und setzen zur Abkürzung:

$$\text{(I.)} \qquad A_i \equiv \cos a_i - \cos a_k \cos a_l - \sin a_k \sin a_l \cos \alpha_i \qquad (i, k, l = 1, 2, 3).$$

Um nun z. B. den Zusammenhang des Sinus-Satzes mit dem Cosinus-Satze deutlich zu erkennen, kann man in verschiedener Weise vorgehen.

Man setze zunächst:

$$B_l \equiv \sin^2 \alpha_i \sin^2 a_k - \sin^2 \alpha_k \sin^2 a_i,$$

so ergiebt sich leicht:

$$\text{(II.)} \qquad B_l \sin^2 a_l \equiv F(A_i, A_k),$$

wo F eine mit den A gleichzeitig verschwindende ganze rationale Function zweiten Grades der A ist, deren Coefficienten ganze rationale Functionen der $\sin a_i$, $\cos a_i$ sind; es giebt nur eine Darstellung dieser Art.

In der That zeigen die üblichen Ableitungen, dass sich der Sinus-Satz zuvörderst in der doppeldeutigen Gestalt

$$\sin \alpha_i \sin a_k = \pm \sin \alpha_k \sin a_i$$

zeigt, und dass die Reduction auf das positive Vorzeichen erst in Folge gewisser Realitätsforderungen (Determinationen) eintritt.

Man kann aber auch von vornherein die Bildung

$$B_l' \equiv \sin \alpha_i \sin a_k - \sin \alpha_k \sin a_i$$

direct untersuchen; das Product $B_l' \sin a_l$ genügt dann einer Gleichung von der Form:

$$\text{(II}'.\text{)} \qquad (B_l' \sin a_l)^4 + (B_l' \sin a_l)^2 \, G(A_i, A_k) + H(A_i, A_k) = 0,$$

wo G, H in obigem Sinne ganze rationale Functionen der A (vom zweiten resp. vierten Grade) sind.

Der Ausdruck B_l' tritt also als irrationale algebraische Function der A auf.

Ein noch einfacheres Beispiel wird durch den bekannten Ausdruck

$$C_{ik} \equiv \cos a_i \sin a_l - \sin a_k \cos \alpha_i - \sin a_i \cos a_l \cos \alpha_k$$

geliefert; man erhält

$$\text{(III.)} \qquad C_{ik} \sin a_l \equiv A_i + A_k \cos a_l.$$

Zwischen den C besteht die wichtige numerische Identität

$$\Sigma(C_{ik}^2 - C_{ki}^2) \equiv 0.$$

Um weiter die Delambre-Gauss'schen Gleichungen richtig zu würdigen, setze man $(i = 1, 2, 3)$

$$E_{i1} \equiv \sin^2 \frac{a_i}{2} \cos^2 \frac{\alpha_k - \alpha_l}{2} - \sin^2 \frac{\alpha_i}{2} \sin^2 \frac{a_k + a_l}{2}$$

und ähnlich E_{i2}, E_{i3}, E_{i4}.

Die E sind irrationale Functionen zweiten Grades der A. Zwischen den zwölf Ausdrücken E bestehen sechs numerische Identitäten, wovon drei einfach lauten:

$$E_{i1} + E_{i2} + E_{i3} + E_{i4} \equiv 0,$$

während die drei weiteren vom zweiten Grade in den E sind. Der in den Delambre-Gauss'schen Formeln hervortretende Dualismus lässt sich hier folgendermaassen kennzeichnen. Versteht man unter den A_i die zu den A_i (I.) dualistischen Ausdrücke (die also aus den A durch Vertauschung der a_i mit den α_i hervorgehen), so ergiebt sich:

$$E_{i1} + E_{i2} \equiv A_i, \quad E_{i1} + E_{i3} \equiv A_i,$$

während jedes einzelne E eine numerische irrationale Function zweiten Grades der sechs Grössen A, A wird.

Dieselbe Fragestellung lässt sich für jede Formel der sphärischen Trigonometrie formuliren: allerdings stehen einer expliciten Durchführung in dem letzteren Sinne erhebliche Schwierigkeiten entgegen.

Bemerkungen zu Kronecker's Theorie der Charakteristiken von Functionen-Systemen.

Von

Walther Dyck (München).

Es handelte sich in dem Vortrage um die besondere Gestaltung, welche die Theorie bei Zugrundelegung specieller Functionensysteme erfährt.

Insbesondere wurde das System von m von einander unabhängigen Functionen

$$f_1, f_2, \ldots, f_m$$

von m+n Variablen $x_1, x_2, \ldots, x_{m+n}$, in Verbindung mit den daraus abgeleiteten Functionen

$$\begin{array}{l} f_{11}+\lambda_2 f_{22} \quad +\cdots+\lambda_m f_{m1}, \\ f_{12}+\lambda_2 f_{22} \quad +\cdots+\lambda_m f_{m2}, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ f_{1\,m+n}+\lambda_2 f_{2\,m+n}+\cdots+\lambda_m f_{m\,m+n}, \end{array}$$

(in welchen die zweiten Indices der f die partiellen Ableitungen nach den Variablen x_i, die λ weitere m—1 Variable bezeichnen) besprochen. Die ausgeführten Untersuchungen werden in den mathematischen Annalen zur Veröffentlichung gelangen.

Anwendungen der Lie'schen Gruppentheorie auf die Dynamik.

Von

P. Stäckel (Halle a. S.).

Eine Methode zur Zerlegung ganzer, ganzzahliger Functionen in irreducible Factoren.

Von

Max Mandl (Prossnitz).

Ist

$$f(x) = c_0+c_1 x+c_2 x^2+\cdots+c_n x^n$$

in das Product

$$(a_0+a_1 x+a_2 x^2+\cdots)(b_0+b_1 x+b_2 x^2+\cdots)$$

zerlegbar, so bestehen zwischen den Coefficienten der gegebenen Function und denen ihrer Factoren Beziehungen von der Form:

$$c_r = \sum_{k=0}^{k=r} a_k b_{r-k} \qquad (r=0, 1, 2, \ldots, n).$$

Der Vortragende zeigt nun, in welcher Weise diese Beziehungen angewendet werden können, um die Coefficienten $a_0, a_1, \ldots; b_0, b_1, \ldots$

in jedem Falle zu ermitteln. — Ergiebt sich gar keine Factorenzerlegung, so ist die vorgelegte Function irreducibel.

Schliesslich wird gezeigt, dass dieselbe Methode auf Functionen von beliebig vielen Variabeln anwendbar ist.

Ueber die Einführung topologischer Gattungsbegriffe in die Lehre von den Verschlingungen

(mit Demonstrationen von Verknüpfungen, Knotenverbindungen und Verknotungen).

Von

O. Simony (Wien).

Ueber ein bei Cauchy'scher Transformation der elliptischen Elementarfunction dritter Art auftretendes Integral.

Von

Mathias Lerch (Prag).

Es sollen die charakteristischen Eigenschaften der durch das Integral

$$\Phi(u, \tau) = \int_{-\infty}^{\infty} e^{\tau x^2 \pi i - 2ux\pi} \frac{dx}{e^{x\pi} + e^{-x\pi}}$$

definirten ganzen transcendenten Function von u, auf welche der Vortragende bei früheren Gelegenheiten geführt worden ist, durch directe Methoden der Integralrechnung begründet werden. Die gemeinten Eigenschaften bestehen in den Beziehungen

$$\Phi(u, \tau) = -\Phi(u+\tau, \tau) e^{-\pi i(2u+\tau)} + e^{-\pi i(u+\frac{1}{4}\tau)}$$
$$= -\Phi(u+1, \tau) + \sqrt{\frac{i}{\tau}}\, e^{\frac{\pi i}{\tau}\left(u+\frac{1}{2}\right)^2};$$

ausser diesen Formeln fanden andere Beziehungen, namentlich die merkwürdige Gleichung:

$$\Phi(u, \tau) = \sqrt{\frac{i}{\tau}}\, \Phi\left(\frac{u}{\tau} \middle| -\frac{1}{\tau}\right) e^{\frac{u^2 \pi i}{\tau}}$$

Erwähnung.

Der Vortrag wird in weiterer Ausführung in den „Monatsheften für Mathematik“ veröffentlicht werden.

Ueber die Erweiterung eines Grundbegriffs der Geometrie der Lage.

Von

Gustav Kohn (Wien).

Nachdem der Vortragende an die Staudt'sche Begriffsbildung des Wurfs von 4 Punkten einer Geraden und deren principielle Bedeutung erinnert hat, erweitert er sie dadurch, dass er allgemein n Elementen eines einförmigen Trägers einen Wurf zuschreibt, den er durch die Festsetzung definirt, dass zwei Reihen von je n Elementen denselben Wurf bestimmen sollen, sobald sie projectiv sind. Die Zweckmässigkeit dieser ungemein nahe liegenden Begriffserweiterung tritt besonders in der Theorie der Collineationen hervor, wo Würfen von mehr als 4 Elementen die Rolle zufällt, welche die vierelementigen Würfe (Doppelverhältnisse) in der Theorie der Homographien inne haben. Als wesentlich erweist sich die vorgenommene Begriffserweiterung aber erst dadurch, dass sie die von den n-elementigen Würfen gebildete Mannigfaltigkeit zum Objecte der geometrischen Untersuchung macht, wodurch, wie der Vortragende an Beispielen zeigt, die Aufmerksamkeit auf neuartige geometrische Theoreme hingelenkt wird. Allgemeine Bemerkungen über mögliche Verallgemeinerungen der besprochenen Begriffsbildung beschliessen den Vortrag. Eine Ausarbeitung desselben erscheint in den Math. Annalen.

Ueber die Beziehung der Kummer'schen Fläche zur projectiven Erzeugung der ebenen Curven vierter Ordnung mit Doppelpunkt.

Von

W. Wirtinger (Wien).

Eine ebene Curve vierter Ordnung mit Doppelpunkt kann bekanntlich auf unendlich viele Arten durch zwei projective Kegelschnittbüschel mit einem gemeinsamen Basispunkt im Doppelpunkt erzeugt werden. Dabei entsteht bei jeder Erzeugung eine Schar corresidualer Tripel auf der C_4, so dass jeder Punkt nur einem Tripel der einzelnen Schar angehört.

Beziehen wir nun zunächst die Strahlen eines Büschels mit dem Scheitel im Doppelpunkt D projectiv auf die Schmiegungsebenen einer

Raumcurve dritter Ordnung R_3 in einem linearen, dreidimensionalen Raume S_3, so bestimmen die drei Strahlen, welche irgend ein Tripel auf C_4 aus D projiciren, einen Punkt in S_3, nämlich den Schnittpunkt der drei Schmiegungsebenen, welche den Strahlen einzeln entsprechen.

Umgekehrt entsprechen aber einem Punkt von S_3 8 Tripel auf C_4, nämlich diejenigen, welche man aus den drei Punktepaaren bilden kann, in welchen die drei Strahlen die C_4 treffen.

Zwei Tripel, die durch Projection aus D aus einander hervorgehen, nennen wir beigeordnet. Einem Punkt in S_3 entsprechen dann 4 Paare beigeordneter Tripel. Die beigeordneten Tripel einer Corresidualschar bilden natürlich wieder eine Corresidualschar.

Den Tripeln einer Corresidualschar entspricht in S_3 eine Curve, welche jede Schmiegungsebene von R_3 zweimal schneidet; denn auf dem entsprechenden Strahl liegen zwei Punkte der C_4, von denen jeder einem und nur einem Tripel der Corresidualschar angehört. Diese Curven sind daher Kegelschnitte. Diese Kegelschnitte berühren sämmtlich jene sechs Schmiegungsebenen von R_3, welche den 6 Tangenten aus D an die C_4 entsprechen, denn für diese fallen die beiden im vorigen erwähnten Tripel immer zusammen.

Zwei beigeordneten Corresidualscharen entspricht dabei immer der nämliche Kegelschnitt.

Umgekehrt entspricht jedem solchen Kegelschnitt ein einziges Paar beigeordneter Corresidualscharen, da durch einen Punkt des Raumes 4 Kegelschnitte hindurchgehen, entsprechend den 4 Paaren beigeordneter Tripel, die einem Punkte von S_3 zugehören.

Man kann nun den einzelnen Corresidualscharen auch die Ebenen der entsprechenden Kegelschnitte zuweisen.

Fasst man nun diese Kegelschnitte zusammen mit ihren Ebenen als die ausgearteten Flächen eines Systems von Flächen zweiter Klasse auf, welche die 6 ausgezeichneten Schmiegungsebenen von R_3 berühren, so ist die von diesen Ebenen umhüllte Fläche die reciproke zu der Kernfläche eines Gebüsches von Flächen zweiter Ordnung mit 6 festen Basispunkten.

Diese ist aber, wie Herr Reye gezeigt hat, eindeutig auf die Kummersche Fläche bezogen, und man kann hieraus die Theorie der Kummerschen Fläche entwickeln.

Es ist also auf geometrischem Wege gezeigt, dass die Punkte der Kummer'schen Fläche auf die Paare beigeordneter Corresidualscharen der ebenen C_4 mit Doppelpunkt eindeutig bezogen sind.

Es hat keine Schwierigkeit, von hier aus zu den Functionen σ und Σ zu kommen, welche Herr Klein eingeführt hat, wenn man die Corresidualschar mit Hülfe von Integralen erster Gattung definirt.

Andrerseits lassen sich Configurationssätze über die Kummer'sche Fläche auf die Tripel übertragen, und umgekehrt.

Z. B. hat Herr Humbert auf Tetraeder aufmerksam gemacht, deren Ecken auf der Fläche liegen, und deren Kanten sie berühren.

Hier erhält man gerade dieselben Tetraeder, wenn man die 4 Paare beigeordneter Tripel betrachtet, welche einem Punkte von S_3 entsprechen. Den 4 dadurch definirten Paaren beigeordneter Corresidualscharen entsprechen auf der Kummer'schen Fläche gerade die Ecken solcher Humbert'scher Tetraeder.

Eine neue Erzeugungsweise des linearen Complexes durch zweimalige Rotation.

Von

Konrad Zindler (Wien).

Wie dieselbe Rotationsfläche durch Rotation einer beliebigen auf ihr liegenden Curve erzeugt werden kann, so lassen sich aus einem linearen Complex verschiedene Strahlencongruenzen herausheben, durch deren Rotation er erzeugt werden kann, und es ist von Interesse, zu untersuchen, ob unter diesen Congruenzen sich solche befinden, die selbst wieder Rotationsgebilde (in Bezug auf eine von der Complexaxe verschiedene Axe) sind:

Denken wir uns zwei congruente Punktfelder, die sich zunächst punktweise decken mögen; wir drehen das eine gegen das andere um einen Punkt 0 um den Winkel ω, heben es dann in der Richtung der gemeinsamen Normalen um die Strecke d ab, wodurch 0 nach $0'$ kommen möge, und verbinden schliesslich je zwei entsprechende Punkte durch eine Gerade. Die Strahlencongruenz $\mathfrak{C}$, die wir so erhalten, ist von der 1. Ordnung und 1. Klasse, denn sie ist das Erzeugnis zweier collinearer Felder, die ihre unendlich ferne Gerade entsprechend gemein haben. Zwei entsprechende Punktreihen in ihnen erzeugen eine Regelschar $\mathfrak{P}$ eines gleichseitig-hyperbolischen Paraboloids mit dem Hauptstrahl $00'$ von $\mathfrak{C}$ als Haupterzeugender. $\mathfrak{C}$ kann offenbar auch durch Rotation von $\mathfrak{P}$ um $00'$ erhalten werden. Der kürzeste Abstand r zwischen $00'$ und einem Strahl von $\mathfrak{P}$ und der Winkel α dieser beiden Geraden stehen, wie eine ein-

fache Rechnung lehrt, in der Beziehung

$$r \cot \alpha = \frac{d}{2} \cot \frac{\omega}{2},$$

die das aus der Theorie der linearen Complexe bekannte Gesetz ausdrückt, da rechts eine constante Grösse steht; u. zw. werden alle Strahlen von $\mathfrak{P}$ einem linearen Complex C angehören, der durch eine in der Mitte von OO' auf OO' und der Richtung jener kürzesten Abstände senkrechte Gerade a als Axe und einen Strahl von $\mathfrak{P}$ als Complexstrahl definirt ist. Aber auch alle übrigen Strahlen von $\mathfrak{C}$ gehören zu C; denn fassen wir die Strahlen von $\mathfrak{C}$ nach Regelscharen $\mathfrak{R}$ von Rotationshyperboloiden zusammen, so gehören von einer beliebigen $\mathfrak{R}$ ausser den beiden Strahlen, die zugleich $\mathfrak{P}$ angehören, auch die zwei zu C, die a schneiden, weil sie auf a senkrecht stehen. Also ist ganz $\mathfrak{R}$ und schliesslich ganz $\mathfrak{C}$ in C enthalten, womit wir eine einfache Erzeugungsweise des linearen Complexes gewonnen haben*):

Man erhält einen linearen Complex, wenn man eine Regelschar eines gleichseitig-hyperbolischen Paraboloids zuerst um ihre Haupterzeugende dreht und dann die so erhaltene Congruenz um eine im Scheitel des Paraboloids auf der Haupterzeugenden senkrechte Gerade sonst beliebiger Richtung rotiren lässt.

Diese beiden Rotationen sind natürlich nicht vertauschbar, da der lineare Complex nur in Bezug auf eine einzige Axe Rotationsgebilde ist.

Ueber einen symbolischen Calcul auf Trägern vom Geschlechte eins.

Von

Emanuel Czuber (Wien).

Zu Beginn dieses Jahres hat ein tragisches Geschick einen hervorragenden Vertreter der synthetischen Geometrie von seinem Schaffen abberufen. Am 25. Januar starb Emil Weyr im besten Mannesalter. Seine letzte Arbeit, die er im Entwurfe zurückliess, galt der Ausbildung einer eigenthümlichen Methode der Untersuchung von Trägern des Geschlechtes

*) Ich habe diese Erzeugungsweise schon im III. Bande der Monatsh. f. Math. und Phys. in der Anm. S. 137 angedeutet.

eins, mit welchen er sich in früheren Abhandlungen wiederholt beschäftigt hatte. Die Methode besteht in einer symbolischen Rechnung mit den Punkten des Trägers. Da der Verstorbene mir die Ausführung und Veröffentlichung dieser seiner Arbeit übertragen hat, so sei es mir gestattet, den Grundgedanken hier mit einigen Worten darzulegen und seine Anwendung an einzelnen Beispielen vorzuführen; dabei soll der einfachste Träger der genannten Art, die ebene Curve dritter Ordnung ohne Doppelpunkt, als Grundlage dienen und mit C_3 bezeichnet werden.

Unter einer Involution nten Grades (n—1)ter Stufe J^n_{n-1} auf C_3 wird die Gesamtheit aller n-gliedrigen Punktgruppen verstanden werden, welche ein gemeinsames Gesetz beherrscht solcher Art, dass durch irgend n—1 Punkte einer Gruppe der nte eindeutig bestimmt ist. Mit einer Gruppe ist die Involution gegeben. Sei $a_1, a_2, \ldots, a_n$ diese Gruppe; dann soll die Zugehörigkeit der allgemeinen Punktgruppe $x_1, x_2, \ldots, x_n$ zu dieser Involution durch die Gleichung

$$x_1 x_2 \ldots x_n = a_1 a_2 \ldots a_n$$

ausgedrückt werden, oder noch einfacher, indem man $a_1 a_2 \ldots a_n = K$ setzt, durch

$$x_1 x_2 \ldots x_n = K.$$

Die Grösse K charakterisirt also die Involution.

Von besonderem Interesse sind jene Punktgruppen, deren Punkte vereinigt liegen; sie ergeben die sogenannten Hauptpunkte der Involution, deren Anzahl n^2 ist; es sind dies die Lösungen der symbolischen Gleichung

$$x^n = K.$$

Die einfachste aller Involutionen ist diejenige Involution dritten Grades, deren Punktgruppen durch die geraden Linien der Ebene ausgeschnitten werden. Sie verdient den Namen der fundamentalen nicht allein deshalb, weil sie mit der Curve selbst schon gegeben ist, sondern auch, wie ich zeigen werde, weil alle anderen Involutionen sich auf sie zurückführen lassen. Die sie charakterisirende Constante heisse k, so dass

$$x_1 x_2 x_3 = k$$

ihre allgemeine Gleichung ist.

Sind x_1, x_2, x_3 drei verschiedene Punkte, so schneidet die zugehörige Gerade die C_3; fallen zwei zusammen, so dass etwa $x_1 = x_2 = x$ und $x_3 = \xi$, so ist die betreffende Gerade Tangente an C_3 im Punkte x, und es bedeutet in der Gleichung

$$x^2 \xi = k$$

ξ den Tangentialpunkt von x; dagegen kann x den Berührungspunkt jeder der vier aus ξ an C_3 gezogenen Tangenten bedeuten. Sind endlich alle

drei Punkte in einen vereinigt, so dass $x_1 = x_2 = x_3 = x$, so ist die betreffende Gerade Wendetangente an C_3 und x ein Wendepunkt; die neun Lösungen der symbolischen Gleichung

$$x^3 = k$$

sind also gleichbedeutend mit den neun Wendepunkten der C_3 als den Hauptpunkten der fundamentalen J_2^3.

Ich habe bereits bemerkt, dass alle Involutionen sich auf die fundamentale zurückführen lassen. Am einfachsten gestaltet sich diese Zurückführung bei denjenigen Involutionen, welche aus C_3 durch Curven einer bestimmten Ordnung ν ausgeschnitten werden; denn dass die so entstandenen 3ν-gliedrigen Punktgruppen eine Involution $J_{3\nu-1}^{3\nu}$ bilden, ist eine Folge des Satzes, dass von den 3ν Schnittpunkten einer C_3 mit einer C_ν jede $3\nu-1$ Punkte den letzten bestimmen. Nun befinden sich unter den C_ν auch Systeme von ν Geraden, in der zugehörigen $J_{3\nu-1}^{3\nu}$ also auch Gruppen von je ν geraden Tripeln, die diese Involution charakterisirende Constante ist daher k^ν. Mithin drückt die Gleichung

$$x_1 x_2 \ldots x_{3\nu} = k^\nu$$

die Thatsache aus, dass die 3ν Punkte $x_1, x_2, \ldots, x_{3\nu}$ der C_3 auf einer Curve νter Ordnung liegen.

Es sei ferner eine J_1^2 durch das Punktepaar a_1, a_2 gegeben; die sie charakterisirende Constante ist

$$K = a_1 a_2;$$

bezeichnet α den dritten Schnittpunkt der Geraden $a_1 a_2$, so ist

$$a_1 a_2 \alpha = k;$$

hieraus folgt $K\alpha = k$ und $K = \frac{k}{\alpha}$; die allgemeine Gleichung dieser J_1^2 lautet also

$$x_1 x_2 = \frac{k}{\alpha}$$

und besagt, in der Form $x_1 x_2 \alpha = k$ geschrieben, dass jedes Punktepaar derselben collinear liegt mit dem Punkte α. So ist jedem Punkte der C_3 eine J_1^2 zugeordnet, sie wird durch die aus diesem Punkte laufenden Strahlen ausgeschnitten.

Eine nichtfundamentale J_2^3 sei durch das Tripel a_1, a_2, a_3 bestimmt; ihre Constante ist

$$K = a_1 a_2 a_3;$$

für den dritten Schnittpunkt b_1 von $\overline{a_2 a_3}$ gilt

$$a_2 a_3 b_1 = k;$$

hieraus ergiebt sich $Kb_1 = ka_1$, woraus $K = \frac{a_1}{b_1} k$, und es lautet die allgemeine Gleichung dieser J_2^3:

$$x_1 x_2 x_3 = \frac{a_1}{b_1} k.$$

Die durch das Quadrupel a_1, a_2, a_3, a_4 bestimmte J_3^4 hat zur Constanten

$$K = a_1 a_2 a_3 a_4;$$

nennt man α den dritten Schnittpunkt von $\overline{a_1 a_2}$, β den dritten Schnittpunkt von $\overline{a_3 a_4}$, endlich γ den dritten Schnittpunkt von $\overline{\alpha\beta}$, so bestehen die Relationen

$$a_1 a_2 \alpha = k,$$
$$a_3 a_4 \beta = k,$$
$$k = \alpha\beta\gamma;$$

aus allen zusammen folgt $K = k\gamma$; der Punkt γ heisst der Gegenpunkt des Quadrupels a_1, a_2, a_3, a_4 und hängt nicht davon ab, wie man die Punkte des Quadrupels zu zwei Paaren verbunden hat. Die allgemeine Gleichung

$$x_1 x_2 x_3 x_4 = k\gamma$$

der J_3^4 drückt also aus, dass diese Involution aus allen Quadrupeln besteht, welche denselben Gegenpunkt γ haben, und so ist jedem Punkte der C_3 eine J_3^4 zugeordnet.

Eine J_4^5 sei durch a_1, a_2, a_3, a_4, a_5 gegeben, so dass

$$K = a_1 a_2 a_3 a_4 a_5$$

die sie charakterisirende Constante ist; durch die fünf Punkte ist ein Kegelschnitt bestimmt, welcher die C_3 in α zum letzten Male schneiden möge; dann ist

$$a_1 a_2 a_3 a_4 a_5 \alpha = k^2$$

und daher $K\alpha = k^2$, mithin $K = \frac{k^2}{\alpha}$. Die allgemeine Gleichung

$$x_1 x_2 x_3 x_4 x_5 = \frac{k^2}{\alpha}$$

dieser J_4^5, in der Form $x_1 x_2 x_3 x_4 x_5 \alpha = k^2$ geschrieben, besagt, diese Involution werde durch die den Punkt α enthaltenden Kegelschnitte ausgeschnitten; α heisst das Centrum der Involution.

Führt man die Betrachtung weiter, so zeigt sich, dass man allgemein eine Involution vom Grade $n = (3\nu + \rho)$ in einer der vier Formen

$$x_1 x_2 \ldots x_n = k^\nu,$$

$$x_1 x_2 \ldots x_n = \frac{\alpha}{\beta} k^\nu,$$

$$x_1 x_2 \ldots x_n = k^\nu \alpha,$$

$$x_1 x_2 \ldots x_n = \frac{k^{\nu+1}}{\alpha}$$

darstellen kann; die beiden ersten Formen entsprechen dem Fall $\rho = 0$, die dritte $\rho = 1$, die letzte $\rho = 2$.

Diese Erörterungen genügen, um beispielsweise die Beziehungen zwischen der C_3 und den sie berührenden Kegelschnitten zu untersuchen.

Es sei x ein Punkt der C_3; der hier zweipunktig berührende Kegelschnitt begegne der Curve ausserdem in den Punkten x_1, x_2, x_3, x_4; dann ist

$$x^2 x_1 x_2 x_3 x_4 = k^2;$$

bezeichnet man ferner mit ξ den Tangentialpunkt von x, so gilt

$$k = x^2 \xi;$$

aus beiden Gleichungen zusammen folgt

$$x_1 x_2 x_3 x_4 = k \xi.$$

Die Schnittreste der ∞^3 die C_3 in x zweipunktig berührenden Kegelschnitte bilden eine Involution vierten Grades, deren Quadrupel den Tangentialpunkt ξ von x zum gemeinsamen Gegenpunkt haben.

Wenn man daher aus ξ eine beliebige Gerade $\xi\alpha\beta$ und durch α, β wieder je eine beliebige Gerade zieht, so bestimmen diese letzteren ein Quadrupel der verlangten Art.

Für den die C_3 in x dreipunktig berührenden Kegelschnitt, welcher weiter in den Punkten x_1, x_2, x_3 schneiden möge, hat man die Gleichung

$$x^3 x_1 x_2 x_3 = k^2$$

und für den Tangentialpunkt ξ von x die weitere

$$k = x^2 \xi;$$

aus beiden ergiebt sich

$$x x_1 x_2 x_3 = k \xi.$$

Die Schnittreste der ∞^2 die C_3 in x dreipunktig berührenden Kegelschnitte bilden eine Involution dritten Grades, deren Tripel durch den Punkt x zu Quadrupeln ergänzt werden, welche den Tangentialpunkt ξ von x zum gemeinschaftlichen Gegenpunkt haben.

Zieht man also durch ξ einen beliebigen Strahl $\xi\alpha\beta$, verbindet einen

der Punkte α, β, z. B. α, mit x und zieht durch den anderen, β, eine beliebige Gerade, so erhält man ein Tripel von der verlangten Art.

Schneidet der in x vierpunktig berührende Kegelschnitt weiter in x_1, x_2, so besteht die Relation

$$x^4 x_1 x_2 = k^2;$$

bezeichnet ferner ξ den ersten, ξ' den zweiten Tangentialpunkt von x, so ist

$$k = x^2 \xi,$$
$$\xi^2 \xi' = k;$$

multiplicirt man die drei Gleichungen, nachdem man die mittlere ins Quadrat erhoben, so entsteht

$$x_1 x_2 \xi' = k.$$

Die Schnittreste der ∞^1 die C_3 in x vierpunktig berührenden Kegelschnitte bilden eine Paarinvolution, deren Centrum der zweite Tangentialpunkt ξ' von x ist.

Jeder durch ξ' geführte Strahl bestimmt also ein Punktepaar von der verlangten Art. Insbesondere aber führen die Tangenten aus ξ' zu vier Kegelschnitten, welche einmal vierpunktig und einmal zweipunktig berühren; von diesen ist jedoch einer, die doppelt gelegte Tangente in x, ein uneigentlicher, so dass sich unter den ∞^1 in x vierpunktig berührenden Kegelschnitten drei befinden, welche an einer anderen Stelle zweipunktig berühren.

Der Kegelschnitt, welcher C_3 in x fünfpunktig berührt, schneide die Curve zum letzten Male in x_1; dann ist

$$x^5 x_1 = k^2;$$

für den ersten und zweiten Tangentialpunkt von x gelten wieder die Gleichungen

$$k = x^2 \xi,$$
$$\xi^2 \xi' = k,$$

und wenn man diese drei Gleichungen in derselben Weise combinirt, wie vorhin, so entsteht die Relation

$$x x_1 \xi' = k.$$

Der einzige Kegelschnitt, welcher die C_3 im Punkte x fünfpunktig berührt (osculirt), schneidet sie dort, wo sie von der Verbindungslinie zwischen x und seinem zweiten Tangentialpunkt getroffen wird.

Auch die von Steiner im 32. Bande des Crelle'schen Journals behandelte Frage nach den besonderen Punkten der Curve, zu welchen

es sechspunktig berührende (superosculirende) Kegelschnitte giebt, lässt sich mit den hier angegebenen Hülfsmitteln erledigen. Für einen solchen besteht die Gleichung

$$x^6 = k^2,$$

welche die 36 Hauptpunkte der durch k^2 charakterisirten Involution sechsten Grades definirt. Unter diesen aber befinden sich auch die Inflexionspunkte als Hauptpunkte der fundamentalen Involution dritten Grades; ist nämlich i ein solcher, so ist $i^3 = k$ und daher auch $i^6 = k^2$; in der That können die doppelt gelegten Inflexionstangenten als degenerirte, sechspunktig berührende Kegelschnitte angesehen werden. Nach ihrer Ausscheidung verbleiben also 27 eigentliche Kegelschnitte. Um diese näher zu bestimmen, bezeichne ι einen der drei Punkte, welche i zum Tangentialpunkt haben; damit ist

$$\iota^2 i = k;$$

daraus folgt durch Erhebung in die dritte Potenz

$$\iota^6 i^3 = k^3$$

und weiter wegen $i^3 = k$

$$\iota^6 = k^2;$$

es ist also ι eine Lösung der obigen Gleichung.

Die gesuchten Punkte sind also die 9×3 Berührungspunkte der aus den Inflexionspunkten an die Curve gezogenen Tangenten; und weil nur drei Inflexionspunkte reell sind, so sind auch nur $3 \times 3 = 9$ von den 27 sechspunktig berührenden Kegelschnitten reell.

Für die Berührungspunkte x_1, x_2, x_3 eines dreimal zweipunktig berührenden Kegelschnitts muss die Gleichung bestehen

$$x_1^2 x_2^2 x_3^2 = k^2;$$

bezeichnet man mit ξ_1, ξ_2, ξ_3 ihre Tangentialpunkte, so hat man

$$k = x_1^2 \xi_1,$$
$$k = x_2^2 \xi_2,$$
$$k = x_3^2 \xi_3;$$

und durch Multiplication aller vier Gleichungen ergiebt sich

$$\xi_1 \xi_2 \xi_3 = k.$$

Die Tangentialpunkte von x_1, x_2, x_3 liegen also in einer Geraden.

Wenn man umgekehrt aus den Punkten eines geraden Tripels die Tangenten zieht, so lassen sich aus den 3 Quadrupeln von Berührungspunkten $4^3 = 64$ Tripel derart zusammenstellen, dass jeder Punkt einem

anderen Quadrupel angehört; nach einem Satze Schröter's, der mit den hier gebotenen Mitteln leicht zu erweisen ist, sind 16 dieser Tripel gerad, die übrigen 48 bestimmen ebenso viele dreimal zweipunktig berührende Kegelschnitte.

Endlich seien x_1, x_2 die Berührungspunkte eines zweimal dreipunktig berührenden Kegelschnitts; für sie muss die Gleichung bestehen

$$x_1^3 x_2^3 = k^2,$$

und für ihre Tangentialpunkte ξ_1, ξ_2 gilt

$$k = x_1^2 \xi_1,$$
$$k = x_2^2 \xi_2;$$

aus allen drei Gleichungen folgt

$$x_1 x_2 = \xi_1 \xi_2.$$

Es gehören also ξ_1, ξ_2 derselben Paarinvolution an wie x_1, x_2. Aber nicht jeder Punkt der C_3 ist Centrum einer solchen Paarinvolution, vielmehr kommt diese Eigenschaft nur den Wendepunkten zu. Denn aus

$$x_1 x_2 o = k$$

ergiebt sich durch Cubirung

$$x_1^3 x_2^3 o^3 = k^3,$$

und soll $x_1^3 x_2^3 = k^2$ sein, so muss

$$o^3 = k;$$

dadurch aber ist o als Inflexionspunkt gekennzeichnet. Hieraus folgt: Jeder durch einen Inflexionspunkt gezogene Strahl schneidet die Cnrve in zwei Punkten, in welchen sie von einem Kegelschnitt je dreipunktig berührt wird.

Es sei mir schliesslich gestattet, zu bemerken, dass Weyr's posthume Arbeit im Band CIII, 2. Abth., der Sitzungsberichte der Wiener Akademie erscheint, und dass eine Anwendung, welche ich von seiner Methode auf die Steiner'schen Schliessungsprobleme gemacht habe, in einem der nächsten Hefte des Crelle'schen Journals abgedruckt werden wird.

Mittheilungen über Johann Bolyai.

Von

Fr. Schmidt (Budapest).

Anknüpfend an den Vortrag des Herrn Alex Wassiljef aus Kasan über Lobatschefskij macht der Vortragende die nachfolgenden Mitteilungen über Johann Bolyai's Untersuchungen.

Im Jahre 1867 wurde der Berichterstatter von Hoüel in Bordeaux ersucht, ihm Nachrichten über die beiden Bolyai bezüglich ihres Lebens und ihrer Werke zu verschaffen, und es erschien in Grunert's Archiv, Band 48 die gewünschte Biographie*). — In den Papieren der Bolyai, die erst in den 70er Jahren eingesehen werden konnten, befindet sich ein Brief aus Temesvár vom 3. November 1823 von Johann Bolyai an seinen Vater, in ungarischer Sprache, der folgende Stelle enthält:

„Ich habe mich entschlossen, sobald die Sachen geordnet sind, eine Arbeit über die Parallelen herauszugeben. — Es ist noch nicht abgeschlossen, aber der Weg, den ich eingeschlagen, verspricht gewiss die Erreichung des Ziels, wenn es überhaupt erreichbar ist. — Es ist noch nicht erreicht — aber ich habe Sachen herausgebracht, dass ich selbst darüber erstaunte. — Es wäre ewig schade, wenn sie verloren gingen. — Sie werden dieselben erkennen. Ich kann nur sagen: dass ich aus Nichts eine andere neue Welt geschaffen habe. — Was ich Ihnen bishero gesendet habe, verhält sich wie ein Kartenhaus zu einem Thurme."

In einer späteren Notiz findet sich:

„Erst im Jahre 1823 habe ich dem Wesen nach das Problem durchdrungen, obschon auch nachher noch Vervollkommnungen hinzukamen. — Ich teilte im Jahre 1825 meinem einstmaligen Lehrer, Herrn Johann Walter von Eckwehr (später k. k. General), einen schriftlichen Aufsatz mit, der sich noch in seinen Händen befindet. Auf Veranlassung meines Vaters habe ich meinen Aufsatz in die lateinische Sprache übersetzt, wo selber als Appendix zum ersten Bande des Tentamen 1832 erschien. — Das Tentamen wurde an Gauss eingesendet. — Nach 6 Wochen kam Gauss' Antwort ...." Die gesamten Briefe von Gauss an Wolfgang Bolyai (11 Stück nach einem Briefe von Sartorius von Waltershausen) befinden sich in Göttingen auf der Sternwarte. Seit dem Tode von Sartorius ist Herr Schering der Hüter dieser Correspondenz, deren Veröffentlichung sehr zu wünschen ist.

In eben diesen Schriften befindet sich ein Brief von Gerling aus Marburg vom 31. October 1854, worin derselbe über die Parallelen folgendes an Wolfgang Bolyai schreibt: „Als ich 1820 etwas von meiner Ansicht über Parallelen drucken liess, hatten wir gegen diese Zeit hier einen juristischen Professor Schweikart, welcher ehemals in Charkow gewesen war, und auf ähnliche Ideen gekommen war, indem er ohne

*) Aus dem Leben zweier ungarischer Mathematiker, Johann und Wolfgang Bolyai von Bolya. Grunert's Archiv, Bd. 48. 1867. S. 217—228.

das Euc. Axiom eine Geometrie, die er Astral-Geometrie nannte, in ihren Anfängen entwickelte. Was er mir darüber mitgeteilt, schickte ich Gauss, der . . . . sich über den grossen Gewinn erklärte, der in dem Appendix zu Ihrem Buche dargeboten ist."

Den Abschluss der Arbeiten Wolfgang Bolyai's bildet ein 1851 zu Maros Vásárhely in deutscher Sprache erschienenes Buch mit dem folgenden Titel:

„Kurzer Grundriss eines Versuchs:

I. Die Arithmetik, durch zweckmässig construirte Begriffe, von eingebildeten und unendlich-kleinen Grössen gereinigt, anschaulich und logisch streng darzustellen.

II. In der Geometrie, die Begriffe der geraden Linie, der Ebene, des Winkels allgemein, der winkellosen Formen, und der Krummen, der verschiedenen Arten der Gleichheit u. dgl. nicht nur scharf zu bestimmen, sondern auch ihr Seyn im Raume zu beweisen; und da die Frage, ob zwey von der dritten geschnittene Geraden, wenn die Summe der inneren Winkel nicht = 2R, sich schneiden oder nicht? niemand auf der Erde ohne ein Axiom (wie Euclid das XI) aufzustellen, beantworten wird; die davon unabhängige Geometrie abzusondern; und eine auf die Ja-Antwort, andere auf das Nein so zu bauen, dass die Formeln der letzten, auf einen Wink auch in der ersten gültig seyen.

Nach einem lateinischen Werke von 1829. M. Vásárhely, und ebendaselbst gedruckten ungrischen." —

Das Tentamen samt Appendix wird nach einem Beschlusse der ungarischen Akademie von 1883 aufs neue herausgegeben.

Ueber Congruenzen, welche in Bezug auf einen Primzahlmodul keine Wurzeln besitzen.

Von

K. Zsigmondy (Wien).

Es bezeichne

$$f_m^{(i)}(x) \equiv 0 \pmod p \quad (i = 1, 2, \ldots p^m)$$

die Gesamtheit der nach dem Primzahlmodul p verschiedenen Congruenzen mten Grades, die man erhält, wenn man den Coefficienten der höchsten Potenz von x gleich der Einheit nimmt, alle anderen aber vollständige Restsysteme modulo p durchlaufen lässt.

Ferner soll unter

$$\Phi(f(x))$$

eine solche Function des ganzzahligen Polynoms $f(x)$ verstanden werden, welche an und für sich oder auch bloss in Bezug auf den Modul p ungeändert bleibt, sobald man die Coefficienten von $f(x)$ um ganzzahlige Vielfache von p vermehrt, so dass also die Aequivalenz

$$\Phi(f(x)) \backsim \Phi(g(x))$$

unter der Voraussetzung

$$f(x) \equiv g(x) \pmod p$$

besteht.

Es findet dann die Beziehung

$$\text{(A)} \left\{ \begin{aligned} \sum_{\alpha} \Phi(f_n^{(\alpha)}(x)) \backsim \sum_{i=1}^{p^n} \Phi(f_n^{(i)}(x)) - \sum_{j} \sum_{i=1}^{p^{n-1}} \Phi(\overline{x-j}\, f_{n-1}^{(i)}(x)) + \\ + \sum_{jj'} \sum_{i=1}^{p^{n-2}} \Phi(\overline{x-j}\; \overline{x-j'}\, f_{n-2}^{(i)}(x)) - \cdots + \cdots \end{aligned} \right.$$

statt. Hierin hat sich die Summation nach α über alle diejenigen Werte der Reihe $1, 2, \ldots p^n$ zu erstrecken, für welche die zugehörigen Congruenzen

$$f_n^{(\alpha)}(x) \equiv 0 \pmod p$$

keine Wurzeln besitzen, während die äusseren Summen auf der rechten Seite sich auf die entsprechenden, aus den Elementen $0, 1, \ldots \overline{p-1}$ gebildeten Combinationen ohne Wiederholung zu beziehen haben.

Setzt man in der Relation (A) erstens

$$\Phi(f(x)) = 1,$$

so erhält man die Anzahl der Congruenzen n ten Grades ohne Wurzeln*).

Nimmt man zweitens

$$\Phi(f(x)) = f(x),$$

so erkennt man unschwer, dass die Summe der Congruenzen ohne Wurzeln $\equiv 0 \pmod p$ ist, einige leicht bestimmbare Fälle ausgenommen.

Die Specialisirung endlich

$$\Phi(f(x)) = \omega^{f(x)},$$

wo ω eine $p$te Einheitswurzel, und x eine ganze Zahl bedeutet, ergiebt auf Grund der Irreducibilität der Kreisteilungsgleichung, dass im Falle $n \geqq p$ das System $f_n^{(\alpha)}(x)$ jede der Zahlen $1, 2, \ldots, \overline{p-1}$ gleich oft

*) Vergl. Wiener Sitzungsber. CIII. S. 135.

modulo p erzeugt. Im Falle $n < p$ wird man auf einen Zusammenhang mit der Theorie der nten Potenzreste geführt; doch wurde dies nicht weiter ausgeführt, da über diesen Gegenstand demnächst ein ausführlicher Aufsatz in einer Zeitschrift erscheinen soll.

Neue Herleitung des Kirchhoff'schen Ausdrucks für das Huygens'sche Princip.

Von

A. Gutzmer (Berlin).

Der analytische Ausdruck, den G. Kirchhoff dem Huygens'schen Princip nach jahrelangem Bemühen gegeben und mit Zuhülfenahme einer Function von besonderer Beschaffenheit aus dem Green'schen Satze hergeleitet hat, kann, wie der Vortragende bereits vor mehreren Jahren bemerkt hat, in naturgemässer Weise durch Umformung bezw. Anwendung der bekannten Green'schen Gleichung

$$4\pi V(x_0, y_0, z_0) = \int \left(V \frac{\partial \frac{1}{r}}{\partial n} - \frac{1}{r} \frac{\partial V}{\partial n} \right) ds - \int \frac{1}{r} \Delta V \, d\tau$$

auf die Function

$$V = \varphi\left(x, y, z, t - \frac{r}{a}\right)$$

gewonnen werden. Diese Herleitung hat vor der Kirchhoff's und vor den Beweisen, welche die Herren Beltrami und Maggi gegeben haben, einerseits eine grössere Einfachheit und andererseits den besonderen Vorzug voraus, ohne Herbeiziehung einer Hülfsfunction von hypothetischem Charakter zum Ziele zu führen. Die ausführliche Darstellung ist im Journal für Mathematik, Bd. 114, S. 333—337, veröffentlicht worden.

Zur Theorie der ganzen algebraischen Zahlen.

Von

Georg Landsberg (Heidelberg).

Es sei $G(z) = 0$ eine ganzzahlige irreducibele Gleichung nten Grades mit dem höchsten Coefficienten 1 und ζ eine ihrer Wurzeln, so bildet die

Gesamtheit der ganzen ganzzahligen Functionen von ζ eine Art (Kronecker) oder eine Ordnung (Dedekind) ganzer algebraischer Zahlen. Entnimmt man ihr irgend ν Elemente $(\beta_1, \beta_2, \ldots, \beta_\nu)$, so bilden dieselben, zu einem System vereinigt, einen Divisor oder ein Modulsystem; eine Zahl μ heisse durch den Divisor teilbar, wenn sie in die Form $\mu = \sum_{i=1}^{\nu} v_i \beta_i$ gesetzt werden kann, worin $v_1, v_2, \ldots, v_\nu$ ebenfalls der Art angehörige ganze Zahlen bedeuten*).

Jedes Modulsystem $(\beta_1, \beta_2, \ldots, \beta_\nu)$ kann dadurch, dass man zu β_h die Elemente $\zeta\beta_h, \ldots, \zeta^{n-1}\beta_h$ hinzufügt und sodann das System auf die Mindestanzahl von n Elementen reducirt, in ein äquivalentes „Modulsystem in der Fundamentalform“ verwandelt werden. Die Aufgabe aber, alle Modulsysteme in der Fundamentalform zu finden, welche sich an die Spitze der Theorie der ganzen algebraischen Zahlen stellen lässt, kann auf eine elementare arithmetische Aufgabe zurückgeführt werden. Bezeichnet man nämlich die n Zahlen $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ resp. mit ξ_1, $\xi_2, \ldots, \xi_n$, so hat man n Gleichungen:

$$\zeta\xi_i = \sum_k c_{ik}\xi_k \qquad (i, k = 1, 2, \ldots, n);$$

ist ferner das Modulsystem in der Fundamentalform durch die n Gleichungen:

$$\alpha_i = \sum_k h_{ik}\xi_k \qquad (i, k = 1, 2, \ldots, n)$$

gegeben, und bezeichnet man die von den ganzzahligen Coefficienten c_{ik} und h_{ik} gebildeten quadratischen Systeme mit C und H, so ist das System HCH^{-1} ebenfalls ganzzahlig, und diese Bedingung ist charakteristisch. Hiernach handelt es sich darum, zu dem gegebenen Systeme C alle Systeme H der erwähnten Eigenschaft aufzufinden; die Lösung dieser Aufgabe geht zurück auf das zuerst von Herrn Frobenius (Crelle's J. Bd. 86, S. 146) behandelte Problem: zwei Scharen bilinearer Formen mit gleichen Elementarteilern auf rationalem Wege in einander überzuführen.

---

*) Der so definirte Teilbarkeitsbegriff ist etwas enger als der übliche, kann aber im weiteren Fortgang der Untersuchung mit diesem in Uebereinstimmung gesetzt werden.

Ueber eine Behandlungsweise der Flächen dritter Ordnung.

Von

Emil Waelsch (Brünn).

Auf einer Fläche dritter Ordnung F_3 sei eine Curve dritter Ordnung $\mathfrak{C}_3$ gewählt. In einem Punkte β der $\mathfrak{C}_3$ giebt es eine einzige Tangente der F_3, welche $\mathfrak{C}_3$ noch in einem Punkte α schneidet. Zwischen den Punkten α und β besteht eine eins-vierdeutige Correspondenz, welche durch

$$I(\alpha) = (A\alpha)_1 + B.\alpha_x$$

ausgedrückt werden kann. Hier ist α_x die lineare Form, die zum Punkte α gehört, A und B sind Formen fünfter resp. dritter Ordnung, und $(A\alpha)_1$ ist die erste Ueberschiebung der Formen A und α. $I(\alpha)$ ist die Form vierter Ordnung der vier Punkte β, welche dem Punkte α entsprechen.

Zu jeder F_3, welche durch $\mathfrak{C}_3$ geht, gehört auf diese Weise eine eins-vierdeutige Beziehung, und umgekehrt. Man kann nun Fragen, die sich auf F_3 beziehen, im binären Gebiete des Systems der Formen A und B behandeln.

Durch die Gleichung

$$II(\varphi) = (A\varphi)_2 + 2(B\varphi)_1 + C\varphi,$$

wo C eine lineare Form ist, wird der quadratischen Form φ die cubische Form $II(\varphi)$ zugeordnet. Die Wurzelpunkte von φ liegen auf einer Bisecante der $\mathfrak{C}_3$, die von $II(\varphi)$ in einer Ebene, welche Bisecante und Ebene sich in einem Punkte der F_3 schneiden; es entspricht so jeder Form φ ein Punkt der F_3, und umgekehrt. Die letzte Formel ist das binäre Bild der Erzeugung der F_3 durch drei collineare Ebenenbündel. Die Ebenen $II(\varphi)$ bilden eines dieser Bündel, dessen Centrum auf F_3 variirt, wenn sich die Form C verändert*).

Es giebt sechs lineare Formen $C^{(i)}$ und sechs zugehörige quadratische Formen $\varphi^{(i)}$ (Lamé'sche Polynome zweiter Ordnung), für welche $II(\varphi^{(i)})$ identisch verschwindet; die Bisecanten der Formen $\varphi^{(i)}$ sind Geraden der F_3. Die 15 Punkte $C^{(i)} - C^{(k)}$ der $\mathfrak{C}_3$ liegen auf den einpunktig

*) Die 5 Wurzelpunkte von A sind die Coincidenzpunkte der Correspondenz $I(\alpha)$; daher wird die $\mathfrak{C}_3$ in jedem dieser Punkte von einer Haupttangente der F_3 berührt.

schneidenden Geraden der F_3*). Dies führt zum algebraischen Problem der sechs $C^{(i)}$: Gegeben sind sechs lineare Formen $C^{(i)}$; sechs quadratische Formen $\varphi^{(i)}$ so zu bestimmen, dass die fünf cubischen Formen $\varphi^{(i)}(C^{(i)} - C^{(k)})$ (k fest) ein Büschel bilden.

Ist C eine beliebige lineare Form, so gehen die sechs Ebenen, welche $\varphi^{(i)}$ mit dem Punkt $C^{(i)} + C$ verbinden, durch denselben Punkt der F_3; es ergiebt sich demnach die Erzeugung der F_3 aus drei trilinear auf einander bezogenen Ebenenbüscheln. —

Werden die Coefficienten φ_0, φ_1, φ_2 der Form φ als homogene Coordinaten eines Punktes einer Ebene angesehen, so erscheint die F_3 auf die Ebene abgebildet, da nach Obigem jedem Punkte von F_3 eine Form φ entspricht. Ist Φ die cubische Form, die zu der beliebigen Ebene Φ gehört, so genügen die Formen φ, welche den gemeinsamen Punkten von F_3 und Φ entsprechen, der Gleichung:

$$((II(\varphi), \varphi)_2 . \varphi - \tfrac{2}{3}(\varphi\varphi)_2 . II(\varphi), \Phi)_3 = 0.$$

Dies ist in den Coordinaten φ_0, φ_1, φ_2 die Gleichung einer ebenen Curve dritter Ordnung C_3; variirt Φ, so erhält man die Gleichungen aller ∞^3 C_3 mit sechs gemeinsamen Punkten.

Die Resultante der Formen φ und $II(\varphi)$ giebt, annullirt, die Gleichung des Bildes der $\mathfrak{C}_3$, also einer Curve fünfter Ordnung mit sechs Doppelpunkten**). —

Haben die cubischen Formen Φ der letzten Formel den Linearfactor M gemein, so gehen die entsprechenden C_3 durch einen siebenten Punkt. Demnach scheint die Theorie der ebenen Curven vierter Ordnung und ihrer algebraischen Functionen als abhängig von den binären Formen A, B, C, M. Die C_4 ist das Bild der Umrisscurve der F_3 für das Projectionscentrum M.

Man kann auch den Scheitel des Bündels $II(\varphi)$ als Centrum wählen; dann sind die C_3 mit sieben gemeinsamen Punkten dargestellt durch

$$((II(\varphi), \varphi)_2 . \varphi - \tfrac{2}{3}(\varphi\varphi)_2 . II(\varphi), II(\psi))_3 = 0,$$

wo ψ eine beliebige quadratische Form ist. Somit erscheint die Theorie der C_4 als abhängig von den Formen A, B, C.

---

*) S. „Zur Geometrie der linearen algebraischen Differentialgleichungen etc." Mitteilungen der deutschen math. Gesellschaft zu Prag, 1892.

**) Dies sind Beispiele der Charakterisirung ebener Curvensysteme und Curven besonderer Art durch simultane invariante Bildungen einer quadratischen Form mit anderen Formen.

Sind Φ^1, Φ^2, Φ^3 die Nullebenen dreier Punkte bezüglich des mit $\mathfrak{C}_3$ verbundenen Nullsystems, so ist die Bedingung dafür, dass die drei Punkte ein Tripel conjugirter Pole der F_3 bilden, wenn

$$(\Phi^i \Phi^k)_2 = (ik)$$

gesetzt wird:

$$(II(2\,3),\, \Phi^1)_3 + (II(3\,1),\, \Phi^2)_3 + (II(1\,2),\, \Phi^3)_3 = 0.$$

Wird

$$III(\Phi) = (A\Phi)_3 + 2(B\Phi)_2 + (C\Phi)$$

gesetzt, und ist Φ die cubische Form der Nullebene eines Punktes, so ist

$$2(III(\Phi),\, \Phi)_1 + II(\Phi\Phi)_2$$

die cubische Form seiner Polarebene bezüglich F_3. —

Die vorstehenden Methoden lassen sich für Gebilde in höheren Räumen und für höhere ebene algebraische Curven verallgemeinern.

Ueber die Werthe einer analytischen Function längs einer Kreislinie.

Von

Alfred Tauber (Wien).

Damit Werte $U + Vi$, welche als stetige Function der Bogenlänge längs einer Kreislinie vorgeschrieben sind, die Randwerte einer analytischen Function vorstellen können, ist erforderlich und hinreichend:

1. dass $\dfrac{U(\alpha-\psi)-U(\alpha+\psi)}{\psi}$ an der Stelle $\psi = 0$ gleichmässig integrirbar für alle α ist;

2. dass die Werthe V durch

$$V(\alpha) = \frac{1}{2\pi}\int_0^\pi [U(\alpha-\psi)-U(\alpha+\psi)]\cot\tfrac{1}{2}\psi\, d\psi$$

gegeben sind.

Ueber die mathematische Ausbildung von Versicherungstechnikern.

Von

L. Kiepert (Hannover).

Meine Herren! Es ist in dieser Versammlung schon mehrfach zum Ausdruck gebracht worden, dass die mathematische Forschung sich nicht allzu sehr in's Abstracte verlieren dürfe, sondern dass sie möglichst Fühlung suchen müsse mit den praktischen Anwendungen. Der Professor der Mathematik hat an den Universitäten häufig eine vereinsamte Stellung, weil seine wissenschaftliche Thätigkeit nur als ein geistvoller Sport angesehen wird, der für das praktische Leben geringe oder gar keine Bedeutung habe. Ein ganz anderes Ansehn gewinnt aber der Mathematiker, wenn er seine Wissenschaft zum Mittelpunkte der Anwendungen macht, wenn er die Beziehungen zur Astronomie und Geodäsie, zur Physik und Mechanik pflegt und fördert.

Auch für den Unterricht sind derartige Beziehungen sehr wertvoll, denn die Studirenden werden einem Vortrage, der auf die nützlichen und lehrreichen Anwendungen hinweist, mit grösserem Interesse folgen als den geistvollsten Theorien, über deren Zweck sich der Anfänger keine Rechenschaft geben kann.

Je weiter nun das Gebiet der Anwendungen ausgedehnt wird, desto besser wird es für den Unterricht und für die Wertschätzung der Mathematik sein.

Während die Anwendungen der Mathematik auf die Astronomie und Geodäsie, auf die Physik und Mechanik in umfangreichem Masse an den Universitäten und technischen Hochschulen berücksichtigt werden, sind wunderbarer Weise die Anwendungen auf das Versicherungswesen vollständig vernachlässigt worden. Mir ist es wenigstens nicht bekannt, dass irgendwo regelmässige Vorlesungen darüber gehalten würden.

Und doch sprechen für die Einrichtung von Vorlesungen über Versicherungswesen ausser den bereits angeführten allgemeinen Gesichtspunkten noch mehrere andere Gründe, welche mir besonders wichtig erscheinen.

1. Den Studirenden der Mathematik würde dadurch neben dem Lehrfache auch noch der Eintritt in die Laufbahn eines Versicherungstechnikers eröffnet, und das ist bei den schlechten Aussichten, welche sich den Lehrern zur Zeit bieten, gewiss nicht zu unterschätzen. Aber

auch solche, die in das Lehrfach eintreten, könnten aus ihren versicherungstechnischen Kenntnissen Vorteil ziehen. Sie würden als mathematischer Beirat einer Versicherungsgesellschaft vermutlich eine lohnendere Nebenbeschäftigung finden als durch das Erteilen von Privatunterricht oder durch das Halten von Pensionären. Das trifft auch noch bei den Lehrern zu, welche an kleineren Orten angestellt sind, denn diesen würde ohne Zweifel die Leitung einer der vielen Sterbekassen oder Krankenkassen zufallen, wenn sie sich die dazu erforderlichen versicherungstechnischen Kenntnisse erworben hätten.

Ausserdem werden von derartigen Kassen und von den Aufsichtsbehörden häufig mathematische Gutachten verlangt. Die Zahl der Sachverständigen ist bis jetzt aber so ausserordentlich klein, dass solche Gutachten nur schwer zu beschaffen sind. Auch dadurch würde den nach dieser Richtung ausgebildeten Lehrern ein lohnender Nebenerwerb zufallen.

2. Weit brennender ist die Frage für das Versicherungswesen selbst. Sie wissen, dass die Mitglieder der verschiedenen Versicherungsgesellschaften in Deutschland und Oesterreich nach Hunderttausenden, ja nach Millionen zählen, und dass sich das Vermögen dieser Gesellschaften auf mehr als eine Milliarde beziffert. Bei der ungeheuren Ausbreitung des Versicherungswesens werden sich diese Zahlen binnen kurzer Zeit verdoppeln und verdreifachen. Wo es sich um das Vermögen so vieler Staatsbürger handelt, scheint es doch geboten, irgend welche Einrichtungen zu treffen, damit die Leiter der Versicherungsgesellschaften eine genügende Vorbildung für ihren verantwortungsvollen Beruf erhalten können. Zur Zeit ist aber die Frage: „Wie sind die in leitender Stellung stehenden Versicherungstechniker mathematisch vorgebildet?“ schwer zu beantworten. Soweit sich nicht die Stellen von dem Vater auf den Sohn oder von dem Onkel auf den Neffen vererbt haben, werden es wohl die meisten mathematischen Directoren ebenso gemacht haben wie ich, dass sie sich die erforderlichen Kenntnisse ausschliesslich durch Selbststudium erworben haben. Ich wenigstens hatte während meiner langen Studienzeit niemals Gelegenheit, irgend eine Vorlesung über Versicherungswesen zu hören. Wenn es sich um die Stellung bei einer grossen Versicherungsgesellschaft handelt, so lohnt es sich ja wohl, zu dem etwas beschwerlichen Selbststudium Zuflucht zu nehmen; es tritt dabei nur die Schwierigkeit ein, dass man dieses Selbststudium bereits hinter sich haben muss, ehe man eine solche Stellung antreten kann. Schlimmer steht es bei den kleineren Gesellschaften, bei den vielen Sterbekassen und Kranken-

kassen, die in den meisten Fällen einer sachverständigen Leitung ganz entbehren. Schon aus der willkürlichen Festsetzung der Beiträge und Sterbegelder bezw. Krankengelder kann man ersehen, dass weder bei der Abfassung noch bei der Genehmigung der Statuten ein Sachverständiger mitgewirkt hat. Verderblich wird dabei in vielen Fällen der Umstand, dass solche Kassen in den ersten Jahren nach ihrer Begründung, wo die Sterblichkeit unter den Mitgliedern noch gering ist, scheinbar sehr gute Geschäfte machen, indem zur Auszahlung der Sterbegelder die eingehenden Beiträge nicht verbraucht werden, so dass ein vermeintlicher Ueberschuss verbleibt. Die Sterbegelder werden in Folge dessen erhöht, und die Kasse wird dadurch der Insolvenz mit Sicherheit entgegengeführt. Der Ueberschuss ist nämlich nur ein vermeintlicher, denn die angesammelten Kapitalien decken zumeist nicht einmal die für die Verbindlichkeiten der Kasse erforderliche „Prämienreserve“, so dass kein Ueberschuss, sondern ein Fehlbetrag vorhanden ist. Der Vorstand solcher Kassen kennt aber in den meisten Fällen den Begriff „Prämienreserve“ überhaupt nicht.

Das würde ganz anders werden, wenn die mathematischen Lehrer auf der Universität Vorlesungen über Versicherungswesen gehört hätten und ihre Kenntnisse derartigen Kassen zur Verfügung stellen wollten.

3. Am dringendsten ist aber das Bedürfnis für die Einrichtung von mathematischen Vorlesungen über Versicherungswesen bei den Juristen vorhanden, in deren Händen die Oberaufsicht über die Versicherungsgesellschaften liegt, und die als Richter über Hunderte von Processen in Versicherungsangelegenheiten zu entscheiden haben. Wie ist es einem Juristen möglich, zu beurteilen, ob die Prämienreserve richtig berechnet ist oder nicht, ob in die Bilanz einer Gesellschaft die zutreffenden Zahlen eingestellt sind oder nicht, ob die Gesellschaft überhaupt lebensfähig ist, wenn er nicht weiss, was Prämienreserve ist? Oder, wie kann ein Richter darüber entscheiden, ob der Rückkaufswert einer Versicherung zu hoch oder zu niedrig berechnet ist, wenn er keinen Einblick in diese Berechnung hat?

Da nützen auch die besten sachverständigen Gutachten nichts. Mögen solche Gutachten auch noch so klar abgefasst sein, so kann sie doch in den meisten Fällen nur der verstehen, der bis zu einem gewissen Grade selbst Sachverständiger ist.

Es ist mir ein Beispiel bekannt, wo die Aufsichtsbehörde aus einem vortrefflichen Gutachten gerade das Gegenteil von dem herausgelesen hat, was der Verfasser des Gutachtens gemeint hat. Wenn die Zeit ausreichte, könnte

ich Ihnen erzählen, wie eine der ältesten und angesehensten Gesellschaften an den Rand des Abgrundes gebracht worden ist, weil der Herr Staats-Commissar „Plus“ und „Minus“ mit einander verwechselt hatte.

Diesem Notstande könnte sehr leicht durch die Einrichtung einer kleinen Vorlesung über die mathematischen Berechnungen im Versicherungswesen abgeholfen werden. Durch einen zweistündigen Vortrag während eines Semesters könnte in dieser Beziehung schon viel erreicht werden; die Juristen, welche diesem Vortrag folgten, würden sich mit derartigen Rechnungen wenigstens einigermassen vertraut machen, und die Mathematiker hätten die Grundlage gewonnen, auf der sie dann ihre weitere Ausbildung im Versicherungswesen leicht selbst bewirken könnten.

Ich würde natürlich die Einrichtung einer so kleinen Vorlesung nur als den erwünschten Anfang zu einer planmässigen Ausbildung von Versicherungstechnikern betrachten und will daher mit meinen bescheidenen Wünschen den weitergehenden Bestrebungen gewiss nicht entgegentreten, welche, wie mir in diesen Tagen privatim mitgeteilt worden ist, augenblicklich in Oesterreich auf der Tagesordnung stehen. Diese Bestrebungen waren mir teilweise schon aus einem Aufsatze bekannt, den Herr Dr. Ernst Blaschke in der österreichischen Beamtenzeitung veröffentlicht hat, und in dem er verlangt, dass eine Instanz geschaffen werde, mittels deren es möglich wäre, Mathematiker als Sachverständige in der Lebensversicherung zu prüfen und hiernach staatlich als Sachverständige anzuerkennen. Zu diesem Zwecke stellt Herr Dr. Blaschke unter Hinweis auf die englischen Einrichtungen die folgenden Forderungen:

1. Die Feststellung eines Unterrichtsprogramms für die Vorbereitung auf das Sachverständigenamt,
2. Namhaftmachung einer Schule, an welcher dasselbe zu absolviren wäre,
3. Feststellung der Erfordernisse für Ablegung von Prüfungen, auf Grund deren die Autorisation zu erteilen wäre,
4. Ernennung einer bezüglichen Prüfungs-Commission,
5. eine Verordnung, bezw. ein Specialgesetz, nach welchem gemäss der Erfüllung aller Vorbedingungen seitens des Candidaten die Autorisation ausgesprochen werden könnte.

Im grossen und ganzen schliesse ich mich den Wünschen und auch den sonstigen Ausführungen des Herrn Dr. Blascke an, nur gegen die zweite Forderung muss ich entschieden Stellung nehmen, dass nämlich nur eine solche Schule, für welche, wie ich höre, die technische Hochschule in Wien in Aussicht genommen ist, namhaft gemacht werde; ich

möchte vielmehr den Wunsch aussprechen, dass Einrichtungen zur Ausbildung von Versicherungstechnikern an sämtlichen Universitäten geschaffen würden.

Obgleich ich selbst Professor an einer technischen Hochschule bin und als solcher Vorlesungen über Versicherungswesen gehalten habe, so ist es mir garnicht zweifelhaft, dass die Ausbildung der Versicherungstechniker nicht an die technische Hochschule, sondern an die Universität gehört.

Das folgt schon aus allem, was ich bisher gesagt habe, insbesondere möchte ich aber noch die folgenden Gründe hinzufügen:

1. Wenn es nur auf die Fertigkeit ankäme, Tarife und Prämienreserven auszurechnen, so könnte man dazu, wie ich aus meiner Erfahrung weiss, auch Leute ausbilden, welche eine niedere Schule besucht haben; für den mathematischen Sachverständigen bedarf es aber vor allen Dingen der mathematischen Schulung des Geistes, wie sie nur den Studirenden der Mathematik an den Universitäten geboten wird. Auch das, was der zukünftige Versicherungsdirector ausserdem braucht, findet er im vollen Umfange nur an der Universität. Ausser der Volkswirtschaftslehre und einigen juristischen Vorträgen würden nämlich noch medicinische Vorlesungen in Frage kommen, denn bei der Entscheidung über die Aufnahme neuer Versicherten muss der Director wissen, ob die Krankheiten, welche der Antragsteller überstanden hat, die Lebensdauer verkürzen oder nicht.

2. Die Einrichtung einer Fachschule für Versicherungstechniker an den technischen Hochschulen würde daher nur möglich sein durch die Heranziehung besonderer Lehrkräfte, während an den Universitäten die erforderlichen Lehrkräfte schon bereit sind.

3. An den technischen Hochschulen würden die Vorträge über Versicherungswesen nur von solchen besucht werden, welche von vornherein die Absicht haben, Versicherungstechniker zu werden, denn die anderen Studirenden, mögen sie Architekten oder Ingenieure, Chemiker oder Elektrotechniker sein, haben auch nicht das geringste Interesse für das Versicherungswesen. Sie haben auch gar keine Zeit, ein solches, ihnen ganz fern liegendes Studium zu treiben, da sie so wie so schon durch ihr eigentliches Fach mit 30 bis 40 und mehr Unterrichtsstunden belastet sind.

Ganz anders stellt sich die Sache an den Universitäten, wo die Mathematiker und Juristen an dem Gegenstande das grösste Interesse haben und auch über die Zeit verfügen, um einige Vorlesungen darüber zu hören.

Durch die Einrichtung einer Fachschule an einer einzelnen technischen Hochschule würde der Staat deshalb nur über eine sehr beschränkte Zahl mehr oder weniger handwerksmässig ausgebildeter Versicherungstechniker verfügen; trifft man aber die entsprechenden Einrichtungen an den Universitäten, so wird der Staat die Mehrzahl der mathematischen Lehrer ausser den eigentlichen Versicherungstechnikern als Sachverständige verwenden können.

4. Am meisten muss dem Staate daran gelegen sein, dass auch die Juristen mathematische Vorlesungen über Versicherungswesen hören können, und das ist doch nur möglich, wenn eine solche Fachschule an den Universitäten eingerichtet wird.

Nachdem die Angelegenheit bereits in Fluss gebracht ist, könnte eine vornehme Zurückhaltung der Universitäten auf diesem Gebiete sehr üble Folgen haben. Hat der Staat einmal an einer einzelnen technischen Hochschule eine Fachschule für Versicherungstechniker eingerichtet und mit besonderen Rechten ausgestattet, so ist der richtige Zeitpunkt für die Universitäten verpasst. Durch eine solche Versäumnis würden aber die Vertreter der Mathematik an den Universitäten sich selbst empfindlich schädigen, denn sie würden die günstige Gelegenheit ungenützt lassen, für die Studirenden der Mathematik in vorteilhafter Weise zu sorgen und die Studirenden der Jurisprudenz zu den mathematischen Vorlesungen heranzuziehen. Es gilt also, jetzt schnell zuzugreifen, wenn die Universitäten nicht für immer auf die mathematische Ausbildung der Versicherungstechniker verzichten wollen.

Ueber die Transformationstheorie der elliptischen Functionen.

Von

M. Krause (Dresden).

Der Vortrag wurde auf Wunsch einiger Mitglieder der Vereinigung gehalten und erst in Wien verfasst. Er bewegte sich in dem nachfolgenden Gedankengange.

Die Transformationstheorie der elliptischen Transcendenten ist so alt wie die Theorie dieser Grössen selbst. Sie knüpft an das Problem an, vorgelegte elliptische Integrale durch Einführung neuer Veränderlichen, welche mit der ursprünglichen durch eine rationale Beziehung verbunden sind, in andere elliptische Integrale zu verwandeln, welche vor den vor-

gelegten gewisse Vorzüge besitzen. Schon bei diesen Problemen tritt der Begriff der Modulargleichung auf, und zwar als der einer algebraischen Gleichung, welche zwischen Constanten besteht, die bei dem ursprünglichen und transformirten Integral vorkommen.

Zu gleicher Zeit mit der Umkehrung der elliptischen Integrale und der Einführung der elliptischen Functionen und Thetafunctionen nimmt das Transformationsproblem eine zweite Form an. Beschränken wir uns auf die rationale Transformation, so kann dasselbe so gefasst werden: „Es sollen die hinreichenden und notwendigen Bedingungen dafür aufgestellt werden, dass elliptische Functionen mit dem Argumente u' und dem Modul c sich rational durch elliptische Functionen mit dem Argumente u und dem Modul k darstellen lassen, wobei vorausgesetzt wird, dass zwischen u und u' eine Beziehung von der Form:

$$u' = Mu + N$$

besteht. Im Anschluss an diese Bedingungen sind die Darstellungsformen näher zu untersuchen."

Das Analoge gilt für die Thetafunctionen.

Dieses Transformationsproblem zerfällt in zwei sehr wesentlich von einander verschiedene Teile.

Der erste Teil stellt es als seine Aufgabe hin, die transformirten elliptischen resp. Thetafunctionen durch die ursprünglichen analytisch darzustellen, und zwar für beliebige Werte der Argumente.

Der zweite Teil dagegen stellt es als Aufgabe, die Beziehungen zu untersuchen, die zwischen den mannigfachen in diesen Darstellungsformeln auftretenden Constanten bestehen.

Der erste Teil kann im wesentlichen als gelöst angesehen werden, und es möge in Bezug hierauf nur auf die bekannten Lehrbücher von Königsberger, Briot und Bouquet u. a. verwiesen werden. Der zweite Teil dagegen ist noch ungelöst und hat Anlass zu einer überaus reichen Fülle wertvoller und inhaltreicher Arbeiten gegeben.

Es stellte sich hierbei als eine der wichtigsten Aufgaben diejenige heraus, die algebraischen Relationen zu studiren, die zwischen den ursprünglichen und transformirten Moduln und anderen mit ihnen zusammenhängenden Grössen bestehen.

Dieses Problem erhielt eine ungeahnte Bedeutung, als es Hermite gelang, mit Hülfe der Modulargleichung, die zu der Transformation fünften Grades gehört, die allgemeine Gleichung fünften Grades zu lösen, als ferner vor allem durch die Arbeiten von Hermite und Kronecker sich überaus wichtige Beziehungen zu der complexen Multiplication und der Zahlen-

theorie ergaben. Ein übersichtliches Bild über das nach dieser Richtung hin Geleistete oder doch über einen sehr grossen Teil desselben giebt das vor kurzem erschienene Werk von Weber über elliptische Functionen. Man kann die Form der Untersuchung, wie sie in diesem Werk und den mit ihm zusammenhängenden Arbeiten vorherrscht, füglich eine algebraische nennen, da die Grundlage algebraischer Natur ist, wobei es freilich nicht ausgeschlossen is, dass zahlentheoretische Untersuchungen hineinverflochten werden.

Daneben aber ist in neuerer Zeit eine zweite Art der Behandlung desselben Problems von Wichtigkeit geworden. Dieselbe beruht auf der Thatsache, dass die Grösse k^2, als Function von τ betrachtet, einer Gleichung Genüge leistet:

$$k^2\left(\frac{a\tau+b}{c\tau+d}\right)=k^2(\tau),$$

wobei a, b, c, d gewisse ganze Zahlen bedeuten. Functionen der angegebenen Art wurden mit dem Namen der Modulfunctionen bezeichnet, und es ergab sich die Aufgabe, von Functionalgleichungen ähnlicher Art ausgehend, die Natur der entsprechenden Functionen zu ergründen. Die vollständigste Uebersicht über das nach dieser Richtung hin Geleistete dürfte das Werk der Herren Klein und Fricke über die elliptischen Modulfunctionen geben. Diese Form der Untersuchung kann füglich als eine functionentheoretische bezeichnet werden, da die Principien der Functionentheorie zu der Lösung der einzelnen Probleme führen.

Zu diesen Betrachtungsarten ist aber noch eine dritte hinzugekommen. Zu derselben führen die folgen Erwägungeu. Erstens haben die bisher genannten Methoden das Problem noch nicht lösen können, Transformationsgleichungen für einen allgemeinen Grad herzustellen, zweitens führt der Versuch, die beiden Methoden für den Fall mehrerer Veränderlichen zu verallgemeinern, zu sehr bedeutenden Schwierigkeiten; und endlich drittens tritt als wichtigster Umstand der folgende hinzu. Zwischen der Behandlungsweise des ersten und des zweiten Teiles der Transformationstheorie besteht bei den beiden ersten Methoden ein tiefgehender Unterschied.

Der erste — der allgemeine Teil — basirt oder kann durchweg auf das Hermite'sche Transformationsprincip basirt werden, der zweite — der specielle Teil — dagegen erfordert ganz eigenartige, ebenso mannigfaltige wie schwierige Methoden, die mit denen des ersten in keiner Beziehung stehen; insbesondere ergeben sich die Constantenrelationen nicht als das, was sie sind, als specielle Fälle allgemeiner Formeln. Ein Beispiel dürfte die letzte Bemerkung besonders klar machen. Auch in der gewöhnlichen

Theorie der elliptischen Functionen giebt es Constantenrelationen, vor allem die Gleichung:

$$\vartheta_3^4 = \vartheta_0^4 + \vartheta_2^4.$$

Diese Formel wird als specieller Fall der Formel:

$$\vartheta_3^2 \vartheta_3^2(v) = \vartheta_0^2 \vartheta_0(v) + \vartheta_2^2 \vartheta_2^2(v)$$

oder einer noch allgemeineren angesehen und dürfte schwerlich mit Hülfe der Reihenentwickelungen der Thetafunctionen abgeleitet werden. Ein solches Verfahren würde hier als unnatürlich bezeichnet werden. In der Transformationstheorie ist aber dasselbe vor allem bei Anwendung der algebraischen Methode bisher das massgebende gewesen. Die Transformationsgleichungen werden thatsächlich grossen Teils mit Hülfe der unbestimmten Coefficienten und mit Anwendung der q-Reihen hergestellt.

Unter solchen Umständen drängt sich von selbst die Frage auf, ob es nicht möglich sein sollte, die beiden Teile der Transformationstheorie unter einem Gesichtspunkt zu betrachten, und zwar als weiteren Ausfluss des Hermite'schen Princips, so dass die Constantenrelationen sich als specielle Fälle allgemeinerer Formeln ergeben. Hierbei können wir noch folgendes bemerken. Aus dem Hermite'schen Princip kann bei den gewöhnlichen Functionen das gewöhnliche bekannte Additionstheorem gefolgert werden, welches die unmittelbare Grundlage der gewöhnlichen Theorie bildet — sollte nun nicht ein anderes Additionstheorem gefunden werden können, welches dasselbe für die Transformationstheorie leistet?

Der erste, der nach dieser Richtung hin Versuche angestellt hat, ist Schröter. Es gelang ihm, Additionstheoreme herzustellen, welche durch Specialisirung eine Fülle wichtiger Constantenrelationen ergaben. Der Grund, warum seine Methode auf die Dauer nicht befriedigen konnte, lag darin, dass in seinen Additionstheoremen immer nur Producte von je zwei Factoren enthalten sind, immerhin müssen aber die Schröter'schen Arbeiten als die grundlegenden der dritten Richtung angesehen werden. In anderen Arbeiten finden sich ähnliche Gedankengänge, z. B. in einer Arbeit von Gordan im 66. Bande des Crelle'schen Journals.

Im Jahre 1886 übergab Herr Klein der Leipziger Gesellschaft der Wissenschaften eine Notiz des Referenten, in welcher zuerst ein allgemeines Additionstheorem zwischen Thetafunctionen mit verschiedenen Moduln aufgestellt wurde. Dieses Additionstheorem ist in mehreren Arbeiten des Referenten und der Dissertation von H. Möller weitergeführt und seine Anwendbarkeit auf die Transformationstheorie der elliptischen und hyperelliptischen Functionen nachgewiesen worden. Um zu demselben zu gelangen, genügte es freilich nicht, Thetafunctionen mit verschiedenen Mo-

duln einzuführen, es mussten ausser den gewöhnlichen Charakteristiken auch noch die sogenannten gebrochenen Charakteristiken in Betracht gezogen werden und mit ihnen Functionen von der Form:

$$\vartheta_{\alpha}\left(v+\frac{g}{n}\tau+\frac{h}{n},\ \tau\right)e^{\frac{\pi i g}{n}\left(2v+\frac{2h}{n}+\frac{g\tau}{n}\right)},$$

in denen überdies an Stelle von τ Multipla von τ zu setzen sind.

Es ist das erlaubt, weil diese Functionen vor allem für die Nullwerte der Argumente in engem Zusammenhang mit den gewöhnlichen transformirten Functionen stehen, so dass Relationen zwischen ihnen auch Gleichungen zwischen den letzteren ergeben. Diese Beziehungen sind besonders einfach, wenn $h = 0$ ist, und aus diesem Grunde hat Referent sich im wesentlichen auf diesen Fall beschränkt, wenngleich der allgemeine keine weiteren principiellen Schwierigkeiten irgend welcher Art darbietet.

Diese soeben angedeuteten Additionstheoreme dürften nun dazu dienen, die Transformationstheorie nach der angegebenen Richtung hin zu erweitern. Sie lassen sich unmittelbar auf Functionen mehrerer Veränderlichen ausdehnen, sie ergeben durch Specialisirung allgemeine Beziehungen zwischen den Constanten, die bei verschiedenen, und zwar den vorkommenden Multipla von τ entsprechenden Transformationsgraden auftreten. Wenn diese Relationen auch nicht als Transformationsgleichungen der ursprünglichen Art angesehen werden können, so bilden sie doch einen wichtigen Uebergang zu denselben. Daneben aber erhalten wir diese Transformationsgleichungen selbst, wenn wir die Zahl der von einander verschiedenen Moduln auf zwei beschränken, und zwar auf τ und $n\tau$, und es ist nicht schwer, sie für die einzelnen Grade in grosser Anzahl zu entwickeln, daneben auch einige, die für einen allgemeinen Grad Gültigkeit besitzen. Das allgemeine Problem freilich, wie wir es vorhin für den zweiten Teil der Transformationstheorie skizzirt haben, kann auch bei dieser Methode noch nicht als gelöst bezeichnet werden, da die wenigen allgemeinen Relationen nicht als genügend angesehen werden können. Die Grundlage des Problems kann hierbei als eine zahlentheoretische bezeichnet werden, da die Lösung zu der Untersuchung eines Systemes linearer Congruenzen führt.

Mittlerweile haben andere Autoren, von anderen Gesichtspunkten ausgehend und ohne mit den Arbeiten des Referenten in Beziehung zu treten, Additionstheoreme zwischen Thetafunctionen mit verschiedenen Moduln aufgestellt. Es möge hier nur auf das Werk der Herren Prym und

Krazer verwiesen werden, welches im Jahre 1892 erschien und den Titel führt: „Neue Grundlagen einer Theorie der allgemeinen Thetafunctionen". Dasselbe zerfällt in zwei Abteilungen. In der ersten wird für den Fall von n veränderlichen Grössen ein allgemeines Additionstheorem aufgestellt, welches für den Fall $n = 1$, der hier allein in Frage kommt, von unwesentlichen, schon angedeuteten Verallgemeinerungen abgesehen, mit dem Additionstheorem des Referenten zusammenfällt. Daneben aber ist durch das genannte Werk ein ganz neuer Gesichtspunkt in die Theorie hereingebracht worden. Das Transformationsproblem knüpft zunächst an die gewöhnlichen elliptischen resp. Thetafunctionen an. Nachdem die Einführung der Thetafunctionen mit gebrochener Charakteristik sich als notwendig gezeigt hat, versuchten die genannten Autoren das Problem auch auf diese allgemeinen Functionen auszudehnen. Hierbei zeigte es sich als notwendig, in Bezug auf die sogenannten Transformationszahlen, die bisher immer als ganze Zahlen angenommen worden waren, die erweiterte Annahme zu machen, dass sie gebrochene Zahlen sein können. Es wird dann das so verallgemeinerte Transformationsproblem wieder in zwei Teile zerfallen, in einen allgemeinen und einen speciellen. In der zweiten Abteilung des genannten Werkes nun wird der erste, der allgemeine Teil, zu Ende geführt, der specielle dagegen nicht in Betracht gezogen.

Ueber die auf die Theorie der conformen Abbildung bezüglichen Arbeiten von Lambert, Lagrange und Gauss.

Von

A. Wangerin (Halle a. S.).

W. bespricht die im Titel genannten Arbeiten und entwickelt einige Gesichtspunkte zur Beurteilung der Fortschritte, die wir jedem der genannten Autoren verdanken. W. hält das ungünstige Urteil, welches Jacobi in seinen Vorlesungen über Dynamik über die Arbeit von Gauss gefällt hat, nicht für zutreffend. Bemerkt werden mag noch, dass die Bezeichnung „conform" zuerst von Gauss im ersten Teile seiner „Untersuchungen über Gegenstände der höheren Geodäsie" vorgeschlagen ist.

Bericht
über die wissenschaftlichen Sitzungen
der Deutschen Mathematiker-Vereinigung
während der Jahres-Versammlung zu Lübeck.

Ueber die Begriffsschrift des Herrn G. Peano und meine eigene.

Von

G. Frege (Jena).

Ueber Franz Neumann's mathematische Arbeiten.

Von

A. Wangerin (Halle a. S.).

Der Inhalt dieses Vortrages ist in den Nachruf für Franz Neumann S. 54—68 dieses Jahresberichts aufgenommen worden.

Ueber die Herstellung eines allgemeinen bibliographischen Repertoriums.

Von

Emil Lampe (Berlin).

Im August d. J. versandte das Office international de bibliographie in Brüssel Einladungen zu einer internationalen bibliographischen Conferenz, die in den Tagen vom 2. bis zum 4. September daselbst abgehalten werden sollte. Dem Einladungsschreiben war eine 28 Seiten lange Druckschrift beigelegt mit dem Titel „Sur la création d'un répertoire bibliographique universel", der die folgenden Angaben entnommen sind.

In ähnlicher Weise, wie die Société mathématique de France einen Zettelkatalog über alle seit dem Anfange unseres Jahrhunderts erschienenen mathematischen Abhandlungen zu veröffentlichen im Begriff ist (wovon die ersten hundert Zettel vorgelegt wurden), soll nach einem einheitlichen Plane die Gesamtheit aller Druckschriften katalogisirt, der so hergestellte Katalog — ebenfalls ein Zettelkatalog, und zwar ein nach den Autoren alphabetisch geordnetes Namensverzeichnis und ein systematisch angeordnetes Sachverzeichnis — durch den Druck zugänglich gemacht werden, so dass ein jeder z. B. den zu den eigenen Studien nötigen Block der Zettel beziehen oder einsehen kann.

Als Muster werden die neueren bibliographischen Einrichtungen der Vereinigten Staaten von Nordamerika benutzt, bei denen mehr oder weniger ein einheitlicher Plan aufgestellt ist. Insbesondere wird für die Ordnung des Sachkatalogs die decimale Einteilung empfohlen, welche durch Melvil Dewey erdacht, von der Vereinigung der Bibliothekare der Vereinigten Staaten angenommen und durchgearbeitet und von der Unterrichtsabteilung des Ministeriums in Washington gutgeheissen ist.

Zur Erläuterung dieses Systems diene das in der Druckschrift Mitgeteilte, wonach nur die Ziffern von 0 bis 9 zur Verwendung kommen. Das ganze Gebiet der Druckschriften wird in zehn Klassen geteilt: 0. Allgemeine Werke, 1. Philosophie, 2. Religion, 3. Sociologie, 4. Philologie, 5. Wissenschaften, 6. Angewandte Wissenschaften, 7. Künste, 8. Litteratur, 9. Geschichte.

Jede Klasse zerfällt in 10 Gruppen, die durch eine der Ziffern 0 bis 9 gekennzeichnet werden, als zweite Ziffer hinter der Klassenziffer, z. B.:

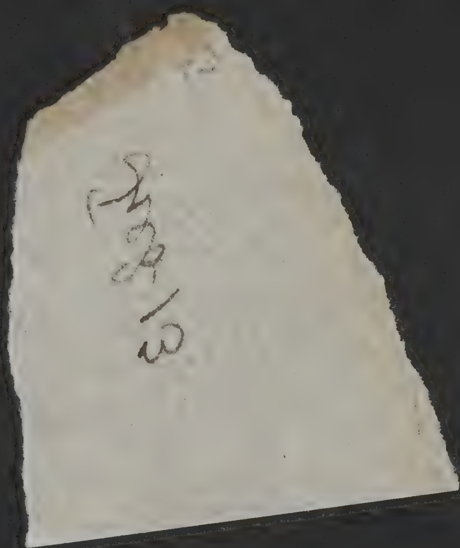
50. Wissenschaften im Allgemeinen, 51. Mathematik, 52. Astronomie, 53. Physik, 54. Chemie, 55. Geologie, 56. Palaeontologie, 57. Biologie, 58. Botanik, 59. Zoologie.

In dieser Weise wird die „Decimalteilung“ fortgesetzt, wofür als weiteres Beispiel die Physik genommen werde:

530. Physik im allgemeinen, 531. Mechanik, 532. Hydraulik, 533. Gase, 534. Akustik, 535. Optik, 536. Wärme, 537. Elektricität, 538. Magnetismus, 539. Molecularphysik.

Der grosse Nutzen eines solchen Katalogs leuchtet unmittelbar ein; vornehmlich würde den einzelnen Bibliotheken ein erhebliches Stück Arbeit abgenommen werden. Zur weiteren Ausbildung des Registers, das den Besitzstand aller Druckschriften gesichert zur Anschauung bringen soll, wird noch eine Bezeichnung vorgeschlagen, die jede einzelne Schrift individuell kennzeichnet. Innerhalb einer Gruppe bilden alle Schriften eines

Feb 13



und desselben Jahres eine Serie, die mit fortlaufenden Zahlen numerirt wird, z. B. in der mit 5253 gekennzeichneten astronomischen Untergruppe erhält im Jahre 1895 ein Artikel die Nummer 12525; dies wird durch den auf dem Zettel verzeichneten Bruch $\frac{12525}{1895}$ angedeutet.

Ein derartiges Unternehmen kann nur durch ein internationales Centralorgan durchgeführt werden, dem die einzelnen Staaten Geldmittel zufliessen lassen. Der Vortragende war verhindert, dem zum Behufe bezüglicher Beratungen stattfindenden Congresse beizuwohnen, hielt es aber für seine Pflicht, den Plan wegen seiner Wichtigkeit in kurzen Umrissen zu skizziren.

Ueber gemeinsame Teiler und gemeinsame Vielfache linearer Differentialausdrücke.

Von

Lothar Heffter (Giessen).

Sind

$$P(y) \equiv p_0 y + p_1 y' + \cdots + p_\nu y^{(\nu)},$$
$$R(y) \equiv r_0 y + r_1 y' + \cdots + r_n y^{(n)}$$

zwei lineare homogene Differentialausdrücke, deren Coefficienten sich bei $x = 0$ rational verhalten, so ist das kleinste gemeinsame Vielfache beider der Differentialausdruck niedrigster Ordnung

$$(1.) \qquad Z \equiv SP \equiv QR,$$

der sowohl durch P als auch durch R teilbar ist. Die Coefficienten der Differentialausdrücke S und Q werden durch Auflösung eines Systems linearer Gleichungen bis auf einen allen gemeinsamen Factor bestimmt.

Es ergiebt sich der Satz: Haben P und R keinen gemeinsamen Teiler, so ist das kleinste gemeinsame Vielfache von P und R genau $(n+\nu)$ter Ordnung, und umgekehrt. — Haben P und R einen grössten gemeinsamen Teiler σter Ordnung, so ist das kleinste gemeinsame Vielfache von P und R von der Ordnung $n+\nu-\sigma$, und umgekehrt.

Die notwendige und hinreichende Bedingung dafür, dass das kleinste gemeinsame Vielfache von niedrigerer als $(n+\nu)$ter Ordnung ist, besteht andererseits in dem identischen Verschwinden einer aus den Coefficienten von P und R gebildeten Determinante, auf die schon in anderer Weise

Herr von Escherich (Denkschriften der Wiener Akademie, Bd. 46, 1883, S. 61 ff.) gekommen ist, und welche die Resultante von P und R genannt wird.

Ein Differentialausdruck P_{-1}, der der Gleichung genügt

(2.) $$P_{-1}P(y) \equiv y + TR(y),$$

heisst zu P mod. R invers; mit seiner Hülfe findet man den zu Q mod. T inversen Differentialausdruck Q_{-1} .

(3.) $$Q_{-1}Q(y) \equiv y + RT(y),$$

und aus diesen beiden Gleichungen (2.) und (3.), sowie aus (1.) folgt

(4.) $$Q_{-1}S \equiv RP_{-1}.$$

Wenn P und R ohne gemeinsamen Teiler sind, gilt das Gleiche von S und P_{-1}, und die Integrale von $R = 0$ und $S = 0$ hängen nach (1.) und (4.) durch die Gleichungen zusammen

(5.) $$y_S \equiv P(y_R)$$

(6.) $$y_R \equiv P_{-1}(y_S).$$

In den vorstehenden Sätzen ist die ganze Theorie der zu derselben Klasse gehörigen Differentialgleichungen enthalten, wie sie im Anschluss an die Riemann'sche Einführung dieses Begriffs von Herrn Fuchs (Sitz.-Ber. d. Berl. Akad., Dec. 1888) entwickelt worden ist. Auch der Satz von Herrn Fuchs, wie die Wurzeln der determinirenden Gleichung durch Uebergang zu einer Differentalgleichung derselben Klasse geändert werden können (Sitz.-Ber. d. Berl. Akad., Nov. 1893), fliesst in denkbar einfachster Weise aus der vorgetragenen Auffassung von Differentialgleichungen derselben Klasse.

(Der Inhalt des Vortrags wird ausführlich an anderer Stelle publicirt werden.)

Ueber infinitesimale Flächendeformationen.

Von

A. Voss (Würzburg).

Wird eine Fläche unendlich wenig deformirt, so existiren bekanntlich in jeder (regulären) Stelle zwei Richtungen, nach denen die Längenelemente ihre Länge nicht ändern, d. h. es gehen durch jeden Punkt im allgemeinen zwei reelle oder imaginäre Curven, die isometrisch deformirt werden, während im singulären Falle diese Doppelschar in eine einzige degenerirt. Ist die Deformation gegeben, so hängt die Be-

stimmung dieser Curven von der Integration einer Differentialgleichung erster Ordnung ab. Anders aber liegt es, wenn man sich die Aufgabe stellt, die Fläche so zu deformiren, dass ein gegebenes Curvensystem isometrisch bleibt. Man wird dann auf eine partielle Differentialgleichung zweiter Ordnung geführt, welche im speciellen wieder auf die der infinitesimalen Biegungsdeformationen der Fläche zurückkommt.

Sind die Punkte der Fläche F durch zwei Parameter μ, ν vermöge der Gleichungen

$$x_{\mu\mu} = A x_\mu + A_1 x_\nu + E p,$$
$$x_{\mu\nu} = B x_\mu + B_1 x_\nu + F p,$$
$$x_{\nu\nu} = C x_\mu + C_1 x_\nu + G p$$

nebst den zwischen den Fundamentalgrössen erster und zweiter Ordnung e, f, g; E, F, G bestehenden Beziehungen ausgedrückt, so hat man im allgemeinen Falle, wo die Curven μ, ν beide isometrisch bleiben sollen, die Componenten ξ, η, ζ einer infinitesimalen Deformation den Bedingungen

$$(1.)\qquad \begin{cases} \Sigma x_\mu \xi_\mu = x_\mu \xi_\mu + y_\mu \eta_\mu + z_\mu \zeta_\mu = 0 \\ \Sigma x_\nu \xi_\nu = x_\nu \xi_\nu + y_\nu \eta_\nu + z_\nu \zeta_\nu = 0 \end{cases}$$

zu unterwerfen. Das heisst, man soll alle Flächen Φ suchen, welche zu F so associirt sind, dass die den Richtungen der Curven $\mu_1(\nu)$ entsprechenden Richtungen auf Φ senkrecht stehen zu den Richtungslinien von $\mu(\nu)$. Im besonderen kann natürlich auch Φ in eine Curve degeneriren, wenn z. B. ξ, η, ζ nur von μ abhängig werden.

Zur Lösung der Gleichungen (1.) führe man zwei charakteristische Functionen φ und ψ ein, vermöge der Gleichungen

$$(2.)\qquad \Sigma x_\mu \xi_\nu = \varphi\sqrt{T}, \quad \Sigma x_\nu \xi_\mu = \psi\sqrt{T}, \quad T = eg - f^2.$$

Alsdann ergeben die Bedingungen der Integrabilität für die ξ, η, ζ zunächst die beiden Gleichungen

$$(3.)\qquad \begin{cases} G\Sigma p\xi_\mu - F\Sigma p\xi_\nu = (\psi_\nu + B(\varphi+\psi))\sqrt{T}, \\ E\Sigma p\xi_\nu - F\Sigma p\xi_\mu = (\varphi_\mu + B'(\varphi+\psi))\sqrt{T}. \end{cases}$$

Ist nun die Fläche F nicht developpabel, so kann man aus (3.) die beiden Grössen

$$\Sigma p\xi_\mu = \Omega_1, \quad \Sigma p\xi_\nu = \Omega_2$$

berechnen und erhält aus der letzten noch zu erfüllenden Integrabilitätsbedingung die Relation

$$(3a.)\qquad \frac{\partial\Omega_1}{\partial\mu} - \frac{\partial\Omega_2}{\partial\nu} = \sqrt{T}(H\varphi - J_1\psi),$$

falls

$$Ff - Eg = HT, \quad Ef - Fe = H_1 T,$$
$$Ef - Fg = JT, \quad Ff - Ge = J_1 T$$

gesetzt wird.

Soll dagegen im singulären Falle das Curvensystem, längs der die μ variabel sind, doppeltzählend isometrisch bleiben, so ist

$$\Sigma x_\mu \xi_\mu = 0, \quad \Sigma x_\mu \xi_\nu + \Sigma x_\nu \xi_\mu = 0$$

zu nehmen. D. h. man kann die Functionen φ und ω durch die Gleichungen

$$(2'.) \quad \Sigma x_\mu \xi_\nu = \varphi\sqrt{T}, \quad \Sigma x_\nu \xi_\mu = -\varphi\sqrt{T}, \quad \Sigma x_\nu \xi_\nu = \omega = \omega'\sqrt{T}$$

einführen und erhält so in analoger Weise:

$$(3'.) \quad \begin{cases} G\Sigma p\xi_\mu - F\Sigma p\xi_\nu = B'\omega - \omega_\mu - \varphi_\nu\sqrt{T}, \\ E\Sigma p\xi_\nu - F\Sigma p\xi_\mu = \varphi_\mu\sqrt{T} - A'\omega, \end{cases}$$

und bei Anwendung derselben Bezeichnungen wie vorhin:

$$(3'a.) \quad \frac{\partial\Omega_1}{\partial\mu} - \frac{\partial\Omega_2}{\partial\nu} = \omega\frac{Ef - Fe}{T} - \varphi\frac{M}{\sqrt{T}},$$

wo

$$M = Eg + Ge - 2fF.$$

Die beiden Gleichungen (3a.), (3'a.) sind Laplace'sche partielle Differentialgleichungen zweiter Ordnung für die unbekannten Functionen φ, ψ, ω. In dem besonderen Falle einer developpabelen Fläche reduciren sich dieselben auf partielle Differentialgleichungen erster Ordnung, die durch blosse Quadratur unmittelbar gelöst werden können, wenn das System der Curven μ aus den Erzeugenden der Fläche besteht. — Setzt man im allgemeinen Falle $\varphi + \psi = 0$, im singulären $\omega = 0$, so hat man die von Herrn Weingarten behandelten infinitesimalen Biegungsdeformationen.

Von den zahlreichen Anwendungen, die sich von diesen Formeln machen lassen, mögen hier nur einige besonders einfache angeführt werden.

1. Die Gleichung (3a.) wird für den Fall, wo die beiden Curven μ, ν Haupttangentencurven von F sind, wie man leicht erkennt,

$$\frac{\partial^2(\varphi - \psi)}{\partial\mu\partial\nu} + B\frac{\partial(\varphi - \psi)}{\partial\mu} + B_1\frac{\partial(\varphi - \psi)}{\partial\nu} = fK(\varphi - \psi),$$

wo K das Krümmungsmass der Fläche bedeutet. Sieht man von der selbstverständlichen Lösung $\varphi = \psi$, welche sich auf den Fall bezieht, wo die Verschiebungsrichtung in der Flächennormalen geschieht, ab, so folgt der Satz:

Die Aufgabe, alle infinitesimalen Deformationen, bei denen das Netz der Haupttangentencurven isometrisch bleibt, zu bestimmen, kommt zurück auf die Ausführung aller infinitesimalen Biegungsdeformationen. Für den singulären Fall, dass nur die eine Schar dieser Curven doppelt zählend isometrisch bleiben soll, findet kein analoges Theorem statt.

2. In dem bereits vielfach behandelten Falle, wo die Normalen der associirten Flächen denen von F in den entsprechenden Punkten parallel bleiben sollen, d. h. wo die Fläche in eine „parallel verlaufende" deformirt werden soll, hat man

$$\Omega_2 = \Omega_1 = 0$$

zu nehmen. Alsdann erhält man, wenn die Fundamentalgrössen von Φ durch angehängte Striche bezeichnet werden, aus (3.), (3a.)

$$E' = \psi \frac{Fe - Ef}{\sqrt{T}}, \quad G' = \varphi \frac{Fg - Gf}{\sqrt{T}},$$

$$F' = \varphi \frac{Eg - Ff}{\sqrt{T}} = \psi \frac{Ge - Ff}{\sqrt{T}},$$

und

$$E'g' + G'e' - 2f'F' = \varphi\psi(\varphi + \psi)F\sqrt{T},$$

mit der Bedingung

$$\frac{\partial^2 l \dfrac{H}{J'}}{\partial\mu\,\partial\nu} + \frac{\partial \dfrac{MB}{H}}{\partial\mu} - \frac{\partial \dfrac{MB'}{J'}}{\partial\nu} = 0.$$

Hieraus folgt: Ist F eine Minimalfläche, also $M = 0$, so muss, falls nicht H und J′ beide Null sind, notwendig $\varphi + \psi = 0$ sein. Soll also eine Minimalfläche so deformirt werden, dass die Normalen in den entsprechenden Punkten parallel bleiben, so kann dies im allgemeinen nur durch Biegung geschehen, und die Fläche Φ ist wieder eine Minimalfläche. Nur wenn für die Curven μ, ν die Gleichungen $H = J' = 0$ erfüllt sind, giebt es auch andere Deformationen; die Fläche Φ ist dann aber auf ein conjugirtes Sytem bezogen. Und umgekehrt: Wird eine Minimalfläche F auf eine beliebige Fläche Φ durch parallele Normalen bezogen, und sind die bei der entsprechenden infinitesimalen Deformation von F isometrisch bleibenden Curven die Curven μ, ν so verschwinden für die letzteren die Grössen H und J′, während das entsprechende System auf Φ ein conjugirtes ist.

In dem singulären Falle hat man dagegen

$$E'f' - F'e' = -\varphi^3 E\sqrt{F},$$
$$E'g' + G'e' - 2f'F' = \varphi^2\omega' E\sqrt{T},$$

also

$$\frac{E'g' + G'e' - 2f'F'}{E'f' - F'e'} = -\frac{\omega'}{\varphi} = -\frac{Eg + Ge - 2fF}{Ef - Fe}.$$

Ist aber F wieder eine Minimalfläche, so muss, falls nicht $Ef - Fe$ gleich Null ist, d. h. das System der (doppeltzählend) isometrisch bleibenden Curven aus den Krümmungscurven einer Schar gebildet ist, auch ω' gleich Null sein, d. h. es ist nur eine Biegung möglich, und auch Φ wird wieder eine Minimalfläche. Ist aber $Ef - Fe = 0$, so wird dem hierdurch bestimmten System von Krümmungslinien ein System von Haupttangentencurven von Φ entsprechen.

Um den Fall der infinitesimalen Paralleldeformation vollständig zu behandeln, ist noch die Möglichkeit zu berücksichtigen, dass die Fläche Φ in eine Curve degenerirt. Alsdann hat man im allgemeinen $\varphi = 0$ zu setzen, d. h. es ist nach (3.), (3a.)

$$Ff - Ge = 0, \quad B' = 0,$$

oder bei gegebenen ξ, η, ζ als Functionen von μ das System der Gleichungen

$$\Sigma x_\mu \xi_\mu = 0, \quad \Sigma x_\nu \xi_\mu = \psi VH,$$
$$\Sigma p \xi_\mu = 0$$

zu lösen. Man hat also zu einer gegebenen Curve ξ, η, ζ alle diejenigen Flächen zu suchen, für welche die Normalen und die Tangenten der Curven μ beständig senkrecht stehen zu den entsprechenden Tangenten dieser Curve.

Die weitere Ausführung übergehend, möge nur noch bemerkt werden, dass im singulären Fall mit $\varphi = 0$ notwendig $f = 0$, $A' = 0$, $e = 1$, $F = 0$ gesetzt werden muss. D. h.: Soll jetzt eine Fläche infinitesimal mit Parallelismus der Normalen so deformirt werden, dass ein doppeltzählendes System isometrisch bleibt, so muss dieselbe eine „surface moulure“ sein.

3. Als ein weiteres Beispiel mögen hier die äquidistanten Transformationen noch angeführt werden. Bei einer solchen Transformation werden alle Flächenpunkte um dieselbe Strecke infinitesimal verschoben. Geometrisch aufgefasst, heisst das, man soll auf einer Kugel alle diejenigen Curvensysteme μ', ν' bestimmen, welche zu den gegebenen Curven-

systemen μ, ν von F bezüglich senkrecht stehen. Man erhält dann unter anderem z. B.:

Alle äquidistanten Transformationen, bei denen die Haupttangentencurven auf einer Fläche isometrisch bleiben, lassen sich unmittelbar aus den Biegungsdeformationen construiren. Soll (im allgemeinen Falle) eine Fläche äquidistant in sich verschoben werden, so muss das Curvensystem μ, ν immer ein solches sein, für das eine der Fundamentalgrössen e, g gleich Eins ist. Nur die developpabelen Flächen lassen äquidistante Transformationen in sich zu, bei denen diese Bedingung nicht erfüllt ist; man erhält sie unmittelbar durch Abwickelung derselben auf die Ebene. Ein ähnliches Resultat ergiebt sich auch für den singulären Fall; die isometrisch bleibenden Curven μ müssen hier geodätische Linien und $e = 1$ sein, wenn die Fläche nicht developpabel ist.

Die weitere Ausführung dieser und einer Reihe von weiteren Fällen (infinitesimale Transformation, bei der die Minimalcurven oder bei denen die Curven eines Orthogonalsystemes etc. etc. isometrisch bleiben) soll einer anderen Mitteilung vorbehalten bleiben.

Würzburg, Anfang October 1895.

Ueber das Additionstheorem der hyperelliptischen Functionen von zwei Argumenten.*)

Von

Peter Pokrowsky (Kiew).

Die allgemeine Form der hyperelliptischen Integrale erster Klasse ist bekanntlich

$$(1.) \qquad \int \tau \, dt,$$

wo τ eine algebraische Function von der Form

$$(2.) \qquad \tau = \frac{f_1(t) + f_2(t)\sqrt{R(t)}}{F_1(t) + F_2(t)\sqrt{R(t)}}$$

*) Der Inhalt dieses Vortrages ist bereits in russischer Sprache publicirt worden (Mathematitschesky Sbornik, Journal der mathemat. Gesellschaft zu Moskau, 1895).

ist. Die Function τ besteht aus den rationalen Functionen f, F und aus dem Polynome fünften Grades $R(t)$; es sei

(3.) $$R(t) = P(t) Q(t),$$

(3′.) $$P(t) = (t - a_1)(t - a_3), \quad Q(t) = (t - a_0)(t - a_2)(t - a_4).$$

Die Function τ hat die Nullstellen n_i, welche durch die Gleichung

(4.) $$f_1^2(t) - f_2^2(t) R(t) = 0$$

gegeben sind; diese Function hat die Unendlichkeitsstellen m_i, welche durch die Gleichung

(5.) $$F_1^2(t) - F_2^2(t) R(t) = 0$$

gegeben sind. Die Function τ hat eben dieselbe Zahl von Nullstellen, wie von Polen: diese Zahl soll nicht kleiner als 3 sein; es ist die Function τ durch die vorausgegebenen Null- und Unendlichkeitsstellen zu bestimmen, aber mit der Bedingung, dass zwei Pole dieser Function (oder zwei Nullstellen) nicht willkürlich sind, sondern sich durch die anderen Null- und Unendlichkeitsstellen ausdrücken lassen.

Es giebt bekanntlich drei Gattungen der hyperelliptischen Integrale; Integrale erster Gattung haben nach Weierstrass die kanonische Form:

(6.) $$J(x, a_{2k-1}) = \int \frac{P(x)\,dx}{2(x - a_{2k-1})\sqrt{R(x)}}, \qquad (k = 1, 2).$$

Aus dem Abel'schen Theoreme erhält man leicht die folgende Additionsformel dieser Integrale:

(7.) $$\sum_i \overset{m_i}{\underset{n_i}{J}} (x, a_{2k-1}) = 0.$$

Mit Hülfe eines besonderen Falles des Abel'schen Theorems für die Integrale zweiter Gattung hat Weierstrass*) eine ganz neue und sehr elegante Lösung des Umkehrproblems gegeben. Die hyperelliptischen Functionen von zwei Argumenten ergeben sich durch die Umkehrung des Systems:

(8.) $$\overset{x_1}{\underset{a_1}{J}}(x, a_{2k-1}) + \overset{x_2}{\underset{a_3}{J}}(x, a_{2k-1}) = u_k, \qquad (k = 1, 2).$$

Die allgemeine Form dieser Functionen ist nach Weierstrass (Zur Theorie der Abel'schen Functionen) folgende:

(9.) $$\frac{\sqrt{(-1)^\alpha (a_\alpha - x_1)(a_\alpha - x_2)}}{\sqrt[4]{(-1)^\alpha R'(a_\alpha)}} = \mathrm{al}(u)_\alpha, \qquad (\alpha = 0, 1, \ldots, 4).$$

(Der Kürze wegen bezeichnen wir die Functionen $\mathrm{al}(u_1, u_2)_\alpha$ durch $\mathrm{al}(u)_\alpha$).

---

*) Vgl. die Weierstrass'schen Arbeiten und Vorlesungen.

Es ist notwendig und hinreichend, nur zwei hyperelliptische Functionen kennen zu lernen; es seien die zwei Functionen durch die Gleichung bestimmt:

$$(10.)\quad (a_{2k-1}-x_1)(a_{2k-1}-x_2)=P'(a_{2k-1})\,.\,b_{2k-1}^2\,.\,\mathrm{al}^2(u)_{2k-1},$$

wo

$$(10'.)\qquad b_{2k-1}^2=\sqrt{\frac{-Q(a_{2k-1})}{P'(a_{2k-1})}}\qquad (k=1,2)$$

ist.

Durch diese zwei Functionen können die anderen Functionen, sowie ihre Differentialquotienten, algebraisch ausgedrückt werden. Es sind nämlich die oberen Grenzen x_1 und x_2 des Systems (8.) die Wurzeln der Gleichung:

$$(11.)\quad (a_3-x)b_1^2\,\mathrm{al}^2(u)_1+(a_1-x)b_3^2\,\mathrm{al}^2(u)_3=P(x).$$

Für die Differentialquotienten bekommt man leicht die folgenden Ausdrücke:

$$(12.)\quad \begin{cases} \dfrac{(a_{2k-1}-x_2)\sqrt{R(x_1)}}{(x_1-x_2)(x_1-a_\alpha)}-\dfrac{(a_{2k-1}-x_1)\sqrt{R(x_2)}}{(x_1-x_2)(x_2-a_\alpha)} \\ \qquad\qquad =P'(a_{2k-1})\dfrac{\partial\log\mathrm{al}(u)_\alpha}{\partial u_k}. \end{cases}$$

Um das Additionstheorem der hyperelliptischen Functionen abzuleiten, construiren wir die Function τ mit den folgenden Nullstellen n_i und Polen m_i:

$$(13.)\quad n_i=a_1^{(4)},\ a_3^{(4)};\quad m_i=a_1,\ a_3,\ x_1,\ x_2,\ y_1,\ y_2,\ z_1,\ z_2.$$

Die Gleichung (5.) wird, nach der Absonderung der Wurzeln a_1 und a_3, durch die folgende ersetzt:

$$(14.)\quad \begin{cases} P(t)[t^2+A_1t+A_0]^2-Q(t)[B_0+B_1t]^2 \\ \qquad =(t-x_1)(t-x_2)(t-y_1)(t-y_2)(t-z_1)(t-z_2). \end{cases}$$

Als nicht willkürliche Pole wählen wir z_1 und z_2; die x_1, x_2, y_1, y_2 sind willkürlich, so wie die entsprechenden Quadratwurzeln aus $R(x)$ und $R(y)$ (bei den letzteren ändern wir die Zeichen). Es ist klar, dass die unbestimmten Coefficienten A_0, A_1, B_0, B_1 aus den vier folgenden Gleichungen zu bestimmen sind:

$$(15.)\quad B_0\sqrt{R(t)}+B_1t\sqrt{R(t)}+A_0P(t)+A_1tP(t)=-t^2P(t),$$

wo man statt t die Grössen x_1, x_2, y_1, y_2 substituirt.

Unter den obengenannten Bedingungen nimmt das Abel'sche Theorem

(Form. 7) die folgende Form an:

$$(16.)\qquad \int_{a_1}^{z_1} J(z, a_{2k-1}) + \int_{a_3}^{z_2} J(z, a_{2k-1}) = u_k + v_k, \qquad (k = 1, 2),$$

wobei:

$$(17.)\qquad \begin{cases} \int_{a_1}^{x_1} J(x, a_{2k-1}) + \int_{a_3}^{x_2} J(x, a_{2k-1}) = u_k, \\ \int_{a_1}^{y_1} J(y, a_{2k-1}) + \int_{a_3}^{y_2} J(y, a_{2k-1}) = v_k. \end{cases}$$

Das Additionstheorem der hyperelliptischen Functionen ist leicht mit Hülfe der Formel (14.) zu erhalten, wenn man $t = a_{2k-1}$ annimmt und nach dem Wurzelausziehen die entsprechenden Functionen (10.) einführt. Dann ergiebt sich leicht:

$$(18.)\qquad b_{2k-1} P'(a_{2k-1}) . D . al(u)_{2k-1} . al(v)_{2k-1} . al(u+v)_{2k-1} = N_{2k-1},$$

wo D und N_{2k-1} die folgenden Determinanten sind:

$$D = \begin{vmatrix} \sqrt{R(x_1)}, & x_1\sqrt{R(x_1)}, & P(x_1), & x_1 P(x_1) \\ \sqrt{R(x_2)}, & x_2\sqrt{R(x_2)}, & P(x_2), & x_2 P(x_2) \\ \sqrt{R(y_1)}, & y_1\sqrt{R(y_1)}, & P(y_1), & y_1 P(y_1) \\ \sqrt{R(y_2)}, & y_2\sqrt{R(y_2)}, & P(y_2), & y_2 P(y_2) \end{vmatrix},$$

$$N_{2k-1} = \begin{vmatrix} (x_1 - a_{2k-1})\sqrt{R(x_1)}, & P(x_1), & x_1 P(x_1), & x_1^2 P(x_1) \\ (x_2 - a_{2k-1})\sqrt{R(x_2)}, & P(x_2), & x_2 P(x_2), & x_2^2 P(x_2) \\ (y_1 - a_{2k-1})\sqrt{R(y_1)}, & P(y_1), & y_1 P(y_1), & y_1^2 P(y_1) \\ (y_2 - a_{2k-1})\sqrt{R(y_2)}, & P(y_2), & y_2 P(y_2), & y_2^2 P(y_2) \end{vmatrix}.$$

Um diese Determinanten durch die hyperelliptischen Functionen darzustellen, benutzen wir die Formel (12.) und die folgenden Relationen:

$$(19.)\qquad \begin{cases} b_1^2(a_3 - x_h)[al^2(u)_1 - al^2(v)_1] + b_3^2(a_1 - x_h)[al^2(u)_3 - al^2(v)_3] \\ \qquad = (x_h - y_1)(x_h - y_2), \end{cases}$$

welche aus der Gleichung (11.) und der analogen für die Argumente v_1 und v_2 entspringen.

Nach einigen Transformationen kommen wir zu dem einfachen Resultat:

$$(20.)\qquad \begin{cases} b_1 W_h^{(1)} al(u+v)_1 + b_3 W_h^{(3)} al(u+v)_3 \\ = b_{2h-1}^2 [al^2(u)_{2h-1} - al^2(v)_{2h-1}], \end{cases} \qquad (h = 1, 2).$$

Die — dem Schöpfer der Methode, Weierstrass, zu Ehren — so

bezeichneten Grössen W haben die Form:

$$W_h^{(2k-1)} = al(v)_{2k-1} \cdot \frac{\partial al(u)_{2k-1}}{\partial u_h} - al(u)_{2k-1} \cdot \frac{\partial al(v)_{2k-1}}{\partial v_h}.$$

Die Formel (20.) ist die unmittelbare Verallgemeinerung des Additionstheorems der elliptischen Functionen. Für diese Functionen in der kanonischen Form von Jacobi haben wir die folgende Formel:

$$W.sn(u+v) = sn^2 u - sn^2 v,$$

wo

$$W = snu \frac{dsnv}{dv} - snv \frac{dsnu}{du}$$

ist.

Zum Schluss mag nebenbei bemerkt werden, dass die Formeln (20.) sehr leicht auf die hyperelliptischen Functionen von mehreren Argumenten zu übertragen sind.

Ueber eine continuirliche Gruppe von Darboux'schen Rotationen.

Von

G. Souslow (Kiew).

1. Die sogenannte Poinsot'sche Bewegung eines starren Körpers lässt sich, wie allgemein bekannt, geometrisch so darstellen: eine fest mit dem Körper verbundene Fläche zweiten Grades

$$(1.) \qquad \frac{x^2}{a} + \frac{y^2}{b} + \frac{z^2}{c} = 1,$$

die ihr Centrum im ruhenden Pole hat, wälzt sich ohne Gleitung auf einer von ihren Tangentialebenen, welche im Raume unbeweglich bleibt; dabei ist immer die Rotationsgeschwindigkeit des Körpers dem Radiusvector des Berührungspunktes proportional. Die Componenten p, q, r der momentanen Rotationsgeschwindigkeit in Bezug auf die Axen der Fläche genügen den Gleichungen:

$$(2.) \quad \frac{dp}{dt} = (x-y)qr; \quad \frac{dq}{dt} = \frac{y-1}{x} rp; \quad \frac{dr}{dt} = \frac{1-x}{y} pq,$$

wo

$$x = \frac{a}{b}; \quad y = \frac{a}{c}.$$

Die vorhergehenden Gleichungen gehören zu dem Typus:

$$(3.)\qquad \frac{dp}{dt} = k_1 qr; \quad \frac{dq}{dt} = k_2 rp; \quad \frac{dr}{dt} = k_3 pq,$$

wo k_1, k_2, k_3 gegebene Constanten sind. Aus (3.) entstehen die Gleichungen (2.), wenn unter den Constanten die Bedingung:

$$(4.)\qquad k_1 + k_2 + k_3 + k_1 k_2 k_3 = 0$$

besteht.

Die Gleichungen (2.) haben zwei algebraische Integrale:

$$(5.)\qquad p^2 + xq^2 + yr^2 = H; \quad p^2 + x^2 q^2 + y^2 r^2 = L^2.$$

Nicht bei allen Werten der willkürlichen Constanten H und L ist unsere Bewegung mechanisch ausführbar; dazu ist notwendig und hinreichend, dass von den drei Producten

$$(6.)\quad (H - L^2)\left(H - \frac{L^2}{x}\right); \quad \left(H - \frac{L^2}{x}\right)\left(H - \frac{L^2}{y}\right); \quad \left(H - \frac{L^2}{y}\right)(H - L^2)$$

zwei negativ sind.

Die Constanten x, y, H, L wollen wir Elemente der Rotation p, q, r nennen, und jetzt gehen wir über zu der ganz elementaren Lösung einer von Herrn Darboux gestellten Aufgabe. Diese Aufgabe lautet so: aus den Elementen einer mechanisch möglichen Poinsot'schen Rotation p, q, r soll man die Elemente einer zweiten Poinsot'schen Rotation π, $\varkappa$, ρ finden, so dass immer folgende Gleichungen bestehen:

$$(7.)\qquad \pi = Ap; \quad \varkappa = Bq; \quad \rho = Cr,$$

wo A, B, C gegebene Constanten sind.

In dem Falle, wenn $A = B = C = -1$, kommen wir zu den sogenannten conjugirten Darboux'schen Rotationen, die eine so grosse Rolle in der Zerlegung der Bewegung des symmetrischen schweren Gyroskops (das Jacobi'sche Theorem) spielen.

2. Die Geschwindigkeiten π, $\varkappa$, ρ müssen den Gleichungen:

$$(8.)\quad \frac{d\pi}{dt} = (\xi - \eta)\varkappa\rho; \quad \frac{d\varkappa}{dt} = \frac{\eta - 1}{\xi}\rho\pi; \quad \frac{d\rho}{dt} = \frac{1 - \xi}{\eta}\pi\varkappa$$

genügen; hier ist $\xi = \frac{\alpha}{\beta}$; $\eta = \frac{\alpha}{\gamma}$; und α, β, γ sind die Quadrate der Halbaxen (mit geeigneten Zeichen) der Fläche zweiten Grades, welche zur geometrischen Darstellung der Bewegung dient.

Es ist von selbst klar, dass die Grössen π, $\varkappa$, ρ nach (7.) Lösungen der Gleichungen des allgemeineren Typus (3.) sind; damit sie aber auch

den Gleichungen (8.) genügen, muss nach (4.) unter den Constanten A, B, C eine Bedingung stattfinden, welche wir so schreiben können:

$$(9.)\quad xy(x-y)l+y(y-1)m+x(1-x)n-lmn(x-y)(x-1)(y-1)=0,$$

indem wir anstatt der Constanten A, B, C drei neue l, m, n, so mit den früheren verbundene:

$$l=\frac{A}{BC};\quad m=\frac{B}{AC};\quad n=\frac{C}{AB},$$

einführen.

Jetzt bemerken wir, dass, wenn A, B, C reell sind, die Constanten l, m, n alle drei dasselbe Zeichen haben müssen.

Aus (9.) sieht man ganz leicht, dass man immer eine zweifache Unendlichkeit von Werten gleichen Zeichens für m und n finden kann, für welche auch l dasselbe Zeichen bekommt, ausser dem Falle, wenn

$$y(x-y)(x-1)<0;\quad x(x-y)(y-1)>0,$$

was von selbst ausgeschlossen ist, da dann $(x-y)^2<0$.

3. Zur Auffindung der Grössen ξ, η haben wir aus (7.) und (8.) folgende Gleichungen:

$$l=\frac{\xi-\eta}{x-y};\quad m=\frac{x(\eta-1)}{\xi(y-1)};\quad n=\frac{y(1-\xi)}{\eta(1-x)},$$

von welchen die erste nach (9.) eine Folgerung der anderen ist. Aus den zwei letzteren finden wir:

$$(10.)\quad \xi=x\frac{y-n(1-x)}{xy-mn(1-x)(1-y)};\quad \eta=y\frac{x-m(1-y)}{xy-mn(1-x)(1-y)}.$$

4. Die algebraischen Integrale der Gleichungen (8.):

$$lp^2+m\xi q^2+n\eta r^2=H'lmn;\quad lp^2+m\xi^2q^2+n\eta^2r^2=L'^2lmn$$

müssen Folgerungen der Integrale (5.) sein. Die Constanten H′ und L′ sind den früheren H, L ganz analog.

Daraus finden wir in bekannter Weise folgende Werte für die zwei noch fehlenden Elemente:

$$lmnH'=\frac{1}{R(y-x)}\{H(myQ-nxP)+L^2(nP-mQ)\},$$

$$lmnL'^2=\frac{1}{R^2(y-x)}\{Hxy(mQ^2-nP^2)+L^2(ynP^2-xmQ^2)\},$$

wo zur Abkürzung gesetzt ist:

$$P=x-m(1-y);\quad Q=y-n(1-x);\quad R=xy-mn(1-x)(1-y).$$

Diese Werte führen uns zu folgenden Gleichungen:

$$(H'-L'^2)\left(H'-\frac{L'^2}{\xi}\right)=\frac{P^2}{lmR^2}(H-L^2)\left(H-\frac{L^2}{x}\right);$$

$$(H'-L'^2)\left(H'-\frac{L'^2}{\eta}\right)=\frac{Q^2}{lnR^2}(H-L^2)\left(H-\frac{L^2}{y}\right);$$

$$\left(H'-\frac{L'^2}{\xi}\right)\left(H'-\frac{L'^2}{\eta}\right)=\frac{1}{mn}\left(H-\frac{L^2}{x}\right)\left(H-\frac{L^2}{y}\right).$$

5. Nach dem Vorhergehenden und nach (6.) können wir jetzt sagen, dass, wenn die gegebene Poinsot'sche Rotation mechanisch ausführbar ist, dann stets auch die gesuchten möglich sind.

Die Ausdrücke (10.) verwirklichen bei constanten Werten von m und n eine eindeutige birationale Transformation der Ebene der Punkte (x, y) in die Ebene der Punkte (ξ, η) mit zwei singulären Punkten (1, 0) und (0, 1). Wenn aber m und n veränderlich sind, so bilden die Grössen ξ, η eine zweigliedrige continuirliche Gruppe.

Geometrische Interpretation des von Sophie Kowalevski behandelten Falles der Bewegung eines schweren starren Körpers um einen festen Punkt.

Von

N. Joukowsky (Moskau).

In der hervorragenden Untersuchung der Bewegung eines schweren starren Körpers, dessen Hauptträgheitsradien a, b, c in Bezug auf den Stützpunkt der Bedingung unterworfen sind, dass

$$a=b=c\sqrt{2}$$

ist, und dessen Schwerpunkt in der Ebene der gleichen Trägheitsradien in der Entfernung X vom Stützpunkte liegt, drückt S. Kowalevski*) alle gesuchten Grössen mit Hülfe zweier Parameter aus, welche hyperelliptische Functionen der Zeit darstellen. Indem ich eine geometrische Interpretation der von ihr untersuchten Bewegung zu geben beabsichtige, möchte ich auf die geometrische Bedeutung der erwähnten Parameter hinweisen.

---

*) S. Kowalevski: „Sur le problème de la rotation d'un corps solide autour d'un point fixe". Acta Mathematica, 12. 2.

Wir untersuchen in der Ebene xoy der gleichen Trägheitsradien (die ox-Axe geht durch den Schwerpunkt des Körpers) die imaginäre Variable

$$\xi = x + yi = r(\cos\varphi + i\sin\varphi)$$

und die Function derselben

$$f(\xi) = -1 + k^2 + l\xi - h\xi^2 + \xi^4 = X + Yi = R(\cos\lambda + i\sin\lambda),$$

wo h, l und k beziehungsweise die Constanten des Integrals der lebendigen Kraft, des Flächenintegrals und die des Integrals bedeuten, welches S. Kowalevski gefunden hat; es bekommt die Totalenergie in Bezug auf die Masse M des Körpers und die Erdbeschleunigung g den Ausdruck $\frac{1}{2}Mg\bar{x}h$ und die Projection des Momentes des impulsiven Kräftepaares auf die Verticale den Ausdruck $\frac{1}{4}Mla\sqrt{2g\bar{x}}$.

Wir setzen:

$$(1.)\qquad \begin{cases} \rho_1 + \rho_2 i = \int \dfrac{d\xi}{\sqrt{f(\xi)}}, \\ \rho_1 - \rho_2 i = \int \dfrac{d\xi_1}{\sqrt{f(\xi_1)}}, \end{cases}$$

worin ξ_1 die zu ξ conjugirte complexe Variable bedeutet, und wollen die Curvenscharen $\rho_1 =$ const. und $\rho_2 =$ const. untersuchen.

Diese Curvenscharen stellen ein isothermisches System der krummlinigen orthogonalen Coordinaten dar. Die Differentialgleichung der Curven $\rho_2 =$ const. ergiebt sich, wenn wir in den Gleichungen (1.) $\rho_2 =$ const. setzen und schreiben:

$$(2.)\qquad \frac{d\xi}{d\rho_1} = \sqrt{f(\xi)}, \quad \frac{d\xi_1}{d\rho_1} = \sqrt{f(\xi_1)}.$$

Nach der Methode von Lagrange*) finden wir für diese Gleichungen (2.):

$$y\frac{d^2x}{d\rho_1^2} - \frac{dx}{d\rho_1}\frac{dy}{d\rho_1} + 4xy^3 = 0.$$

Indem wir mit

$$\frac{2}{y^3}\frac{dx}{d\rho_1}$$

multipliciren und hierauf integriren, erhalten wir:

$$\left(\frac{\frac{dx}{d\rho_1}}{y}\right)^2 + 4x^2 = s_2.$$

*) Oeuvres de Lagrange. T. IX. p. 127.

Die hier auftretende Integrationsconstante s_2 hängt nur von ρ_2 ab. Die Grösse $\frac{s_2}{4}$ stellt einen von den Parametern von S. Kowalevski dar. Den zweiten Parameter $\frac{s_1}{4}$ erhält man in analoger Weise:

$$-\left(\frac{\frac{dx}{d\rho_2}}{y}\right)^2 + 4x^2 = s_1.$$

Da sich aus den Gleichungen (2.) ergiebt, dass

$$(3.)\quad \begin{cases} \dfrac{dx}{d\rho_1} = \sqrt{R}\cos\dfrac{\lambda}{2} = \sqrt{\dfrac{R+X}{2}}, \\ \dfrac{dx}{d\rho_2} = -\dfrac{dy}{d\rho_1} = -\sqrt{R}\sin\dfrac{\lambda}{2} = -\sqrt{\dfrac{R+X}{2}}, \end{cases}$$

so lassen sich die Grössen s_1 und s_2 in folgender Weise durch algebraische Functionen der Coordinaten x, y darstellen:

$$(4.)\quad \begin{cases} s_1 = \dfrac{-R+X}{2y^2} + 4x^2, \\ s_2 = \dfrac{R+X}{2y^2} + 4x^2. \end{cases}$$

Somit ergeben sich s_1 und s_2 als nichtisothermische Parameter des oben erwähnten Coordinatensystems.

Aus den Gleichungen (3.) folgt:

$$\left(\frac{dx}{d\rho_1}\right)^2 + \left(\frac{dx}{d\rho_2}\right)^2 = R,$$

d. h. der erste Differentialparameter der Functionen ρ_1 und ρ_2 lässt sich ausdrücken in der Form:

$$(5.)\qquad \Delta\rho_1 = \Delta\rho_2 = \frac{1}{\sqrt{R}}.$$

Ausserdem folgt aus dieser Gleichung mit Evidenz die Richtigkeit des folgenden Satzes:

Satz I. Die Tangenten der Coordinatencurven $s_1 = \text{const.}$ und $s_2 = \text{const.}$ sind Halbirende der Winkel, welche die Vectoren R mit der ox-Axe bilden.

Es sei hier noch bemerkt, dass der Winkel zwischen der Richtung des Vectors R und der positiven Richtung der ox-Axe (dem Teil der Axe, auf welchem der Schwerpunkt liegt) durch die Curve $s_2 = \text{const.}$ halbirt wird.

Die Gleichungen (5.) geben die Grösse des ersten Differentialparameters der Functionen ρ_1 und ρ_2; was die Functionen s_1 und s_2 anbetrifft, so werden ihre ersten Differentialparameter durch die Gleichungen bestimmt:

$$(6.)\quad \begin{cases} \Delta s_1 = 2\sqrt{\dfrac{(e_1 - s_1)(e_2 - s_1)(e_3 - s_1)}{R}}, \\ \Delta s_2 = 2\sqrt{-\dfrac{(e_1 - s_2)(e_2 - s_2)(e_3 - s_2)}{R}}, \end{cases}$$

worin e_1, e_2, e_3 sich durch die Wurzeln ε_1, ε_2, ε_3, ε_4 der Gleichung $f(\xi) = 0$ (die ihrerseits der Bedingung $\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4 = 0$ genügen) in folgender Weise ausdrücken:

$$e_1 = (\varepsilon_1 + \varepsilon_2)^2, \quad e_2 = (\varepsilon_1 + \varepsilon_3)^2, \quad e_3 = (\varepsilon_1 + \varepsilon_4)^2.$$

Das neue Integral, welches S. Kowalevsky für den untersuchten Fall der Bewegung gefunden hat, leite ich geometrisch ab und stelle es in Form eines Satzes auf. Um diesen Satz übersichtlicher formuliren zu können, wollen wir unter dem Namen eines Doppelvectors des gegebenen Vectors (r, φ) einen solchen verstehen, dessen Länge r^2 und dessen Winkel mit der ox-Axe gleich 2φ ist, und die Einheit der Zeit so wählen, dass

$$\frac{a^2}{2g\bar{x}} = 1.$$

Satz II. Die Entfernung der Endpunkte zweier Vectoren, von denen der erste ein Doppelvector der Projection der Winkelgeschwindigkeit auf die Ebene gleicher Trägheitsradien und der zweite die auf dieselbe Ebene abgebildete Projection der Längeneinheit ist, welche von dem Stützpunkte auf der Verticalen nach oben abgetragen ist, bleibt constant.

Diese Entfernung ist die constante Grösse k. Ich betrachte k als Vector und schreibe ihm eine Richtung vom Endpunkte des Doppelvectors der Projection der Winkelgeschwindigkeit aus zu.

Es sei der Punkt N der Endpunkt der Projection der Winkelgeschwindigkeit auf die Ebene der gleichen Trägheitsradien. Wir wollen ihre Coordinaten durch (x, y) bezeichnen und auf diese alle oben erwähnten Gleichungen beziehen.

Die Bewegung des Punktes N in der xoy-Ebene kann durch den Satz I und den folgenden Satz III bestimmt werden, welcher sich als Folgerung des Integrals der lebendigen Kraft und des Flächenintegrals ergiebt.

Satz III. Der Vector $\frac{R}{4}$ wird nach der Parallelogrammregel aus dem Doppelvector der Geschwindigkeit des Punktes N und des Vectors y^2k, welcher nach k gerichtet ist, gebildet.

Für den gegebenen Punkt N ist der Vector $\frac{R}{4}$ nach Richtung und Grösse vollkommen bestimmt, der Vector y^2k ist der Grösse nach bekannt; was den Doppelvector der Geschwindigkeit v des Punktes N anbelangt, so ist er auch der Grösse nach bekannt und wird durch die Gleichung ausgedrückt:

$$(7.) \qquad 4v^2 = -X + 2hy^2 - 8x^2y^2.$$

Diese Grundlagen erlauben, das in Frage stehende Parallelogramm zu construiren, indem wir ihm zwei Lagen geben können, welche durch Drehung um 180^0 um R in einander übergehen. Indem wir durch 2ϑ und 2χ die Winkel bezeichnen, welche die Diagonale des Parallelogramms mit dessen Seiten v^2 und y^2k einschliesst, können wir die gewöhnlichen trigonometrischen Gleichungen schreiben:

$$\operatorname{tg}\vartheta = \sqrt{\frac{\left(\frac{R}{4} - v^2 + y^2k\right)\left(-\frac{R}{4} + v^2 + y^2k\right)}{\left(\frac{R}{4} + v^2 - y^2k\right)\left(\frac{R}{4} + v^2 + y^2k\right)}},$$

$$\operatorname{tg}\chi = \sqrt{\frac{\left(\frac{R}{4} + v^2 - y^2k\right)\left(-\frac{R}{4} + v^2 + y^2k\right)}{\left(\frac{R}{4} - v^2 + y^2k\right)\left(\frac{R}{4} + v^2 + y^2k\right)}},$$

welche auf Grund der Gleichung (7.) und der Gleichungen (4.) zu der Form führen:

$$(8.) \qquad \begin{cases} \operatorname{tg}\vartheta = \sqrt{-\frac{(s_2 - k_1)(s_2 - k_2)}{(s_1 - k_1)(s_1 - k_2)}}, \\ \operatorname{tg}\chi = \sqrt{-\frac{(s_1 - k_1)(s_2 - k_2)}{(s_2 - k_1)(s_1 - k_2)}}, \end{cases}$$

worin

$$k_1 = h - 2k,$$
$$k_2 = h + 2k$$

ist. Denken wir uns drei Geraden, die die Winkel halbiren, welche die ox-Axe mit den Vectoren $\frac{R}{4}$, v^2, y^2k bildet. Die erste dieser Geraden fällt in die Richtung der Tangente, welche im Punkte N die Coordinaten-

curve $s_2 = \text{const.}$ tangirt, die zweite fällt in die Richtung der Geschwindigkeit v des Punktes N und die dritte in die Richtung des Vectors, von welchem k der Doppelvector ist. Es ist evident, dass die zweite und die dritte Gerade die Winkel ϑ resp. χ mit der ersten bilden.

Somit entsteht eine geometrische Vorstellung von der Bahn des Punktes N. Diese Bahn schneidet die Curvenschar $s_2 = \text{const.}$ unter dem Winkel ϑ, der durch die erste Gleichung (8.) bestimmt ist.

Bei dieser Gelegenheit findet die Duplicität der Lösung darin ihren Ausdruck, dass man den Winkel ϑ nach Belieben nach der einen oder der anderen Seite der Curve $s_2 = \text{const.}$ abtragen kann, was darauf hindeutet, dass die Schar der Bahnen des Punktes N bei gegebenen h, l und k eine Enveloppe besitzen.

Die Differentialgleichung der Bahn des Punktes N in den betrachteten krummlinigen Coordinaten lässt sich schreiben wie folgt:

$$\frac{ds_2}{\Delta s_2} : \frac{ds_1}{\Delta s_1} = \operatorname{tg}\vartheta,$$

was vermittels der Gleichungen (6.) und der ersten Gleichung (8.) zu der Form führt:

$$\frac{ds_2}{\sqrt{S_2}} - \frac{ds_1}{\sqrt{S_1}} = 0, \tag{9.}$$

worin

$$S_1 = (e_1 - s_1)(e_2 - s_1)(e_3 - s_1)(k_1 - s_1)(k_2 - s_1),$$
$$S_2 = (e_1 - s_2)(e_2 - s_2)(e_3 - s_2)(k_1 - s_2)(k_2 - s_2).$$

Wir legen um den Stützpunkt o als Centrum eine Kugeloberfläche mit dem Radius 1 und bezeichnen ihren obersten Schnittpunkt mit der durch o gehenden Verticalen mit H; diese Kugeloberfläche sei mit dem Körper unveränderlich verbunden.

Bei der Bewegung des Körpers beschreibt der Punkt H eine sphärische Curve auf dieser Kugel.

Ist Q die Projection des Punktes H auf die Ebene der gleichen Trägheitsradien, so stellt die Bahn des Punktes Q in dieser Ebene die Projection der erwähnten sphärischen Curve auf dieselbe Ebene dar.

Um die Bahn des Punktes Q zu finden, muss man jeden Radiusvector der Bahn des Punktes N durch seinen Doppelvector ersetzen und durch dessen Endpunkt den Vector k führen. Die Richtungen von k werden vermittelst des Winkels χ aus der zweiten Gleichung (8.) gefunden. Die Endpunkte von k verzeichnen dann die Bahn des Punktes Q.

Die Bewegung des Körpers geht in der Weise vor sich, dass

die mit ihm fest verbundene sphärische Curve über den Punkt H hinweggleitet.

Die Abhängigkeit der Lage des Punktes H auf der sphärischen Curve von der Zeit geht aus der Betrachtung der Bewegung des Punktes N hervor.

Indem wir die Projection der Geschwindigkeit v auf die Coordinatencurven $s_1 = \text{const.}$ und $s_2 = \text{const.}$ zusammenstellen, finden wir:

$$\frac{ds_1}{\Delta s_1\, dt} = v \cos\vartheta, \qquad \frac{ds_2}{\Delta s_2\, dt} = v \sin\vartheta.$$

Auf Grund der ersten Gleichung (8.) und der Gleichungen (6.) lassen sich diese Ausdrücke in folgender Weise umformen:

$$dt = \frac{R}{y^2}\frac{ds_1}{\sqrt{S_1}},$$

$$dt = \frac{R}{y^2}\frac{ds_2}{\sqrt{S_2}}.$$

Indem wir die zweite Gleichung mit s_2, die erste mit s_1 multipliciren und subtrahiren, erhalten wir nach der Division durch

$$s_2 - s_1 = \frac{R}{y^2}$$

die gesuchte Relation zwischen t, s_1, und s_2:

$$(10.) \qquad dt = \frac{s_2\, ds_2}{\sqrt{S_2}} - \frac{s_1\, ds_1}{\sqrt{S_1}}.$$

Um nunmehr die Lage des Körpers vollkommen zu bestimmen, muss man seine Drehung um die Verticale oH ins Auge fassen.

Diese Drehung wird durch den Winkel ψ charakterisirt, welchen die durch oH und oz gehende Ebene mit einer festen durch oH gelegten Ebene bildet.

Der Winkel ψ wird durch die Gleichung gegeben:

$$\frac{d\psi}{dt} = \frac{r\cos(\varphi+\nu)}{\sin\theta},$$

in welcher (r, φ) die Polarcoordinaten des Punktes N, θ den Winkel Hoz und ν den Winkel zwischen dem Vector oQ und dem Doppelvector von r darstellen. Die rechte Seite dieser Gleichung lässt sich leicht durch s_1 und s_2 ausdrücken.

Von der hier dargestellten allgemeinen Theorie mache ich eine Anwendung auf die eingehende Untersuchung der Bewegung des Körpers im Falle $l = 0$ und $k = 0$.

Die Discontinuitätsbereiche der Gruppen reeller linearer Substitutionen einer complexen Veränderlichen.

Von

Robert Fricke (Braunschweig).

Eine Gruppe Γ aus reellen linearen Substitutionen einer complexen Variablen (von Poincaré als Fuchs'sche Gruppe bezeichnet) lässt sich in die Gestalt einer Gruppe von Collineationen transformiren, welche sämtlich eine feste Ellipse C_2 in sich überführen. Ist die Gruppe im Innern der C_2 eigentlich discontinuirlich, so liefert für ihre weitere Behandlung der Begriff des Fundamental- oder Discontinuitätsbereichs (im folgenden durch D. B. bezeichnet) die Basis. Ueber die Gestalt dieser Bereiche sind von Klein und Poincaré wichtige Ansätze entwickelt. Eine abgeschlossene Theorie der D. B. ist neuestens durch den Verf. ausgebildet, und zwar auf Grundlage projectiver Betrachtungen in der Ebene der C_2. Man hat sich dabei der auf die Ellipse C_2 als absolutes Gebilde gegründeten projectiven Maassbestimmung zu bedienen.

Es sind drei wesentlich verschiedene Gestalten von D. B. zu unterscheiden, welche ich als normale, natürliche und kanonische D. B. bezeichne.

Greift man ein particuläres System bezüglich Γ äquivalenter Punkte auf und macht letztere zu Centren gleich grosser Kreise, so werden diese Kreise, wenn die Radien klein genug sind, nicht collidiren. Man lasse nun die Kreise gleichzeitig und gleichmässig wachsen, wobei der einzelne Peripheriepunkt so lange weiter wandern soll, als er noch freies Gebiet antrifft. Der einzelne Kreis wird dabei zu einem Polygon P auswachsen, und es entspringt ein ganzes, zur Gruppe Γ gehörendes Netz von Polygonen P_0, P_1, . . ., welche eben die normalen D. B. darstellen.

Das einzelne Normalpolygon P_0 ist geradlinig begrenzt und hat lauter concave Winkel; es ist mit seinem Centrum eindeutig bestimmt und besitzt eine grosse Reihe weiterer einfacher Eigenschaften. Ist das Geschlecht von Γ mit p bezeichnet, und hat P_0 im ganzen n Ecken, welche Fixpunkte von Substitutionen aus Γ sind, so ist die Seitenanzahl s des Normalpolygons durch $s = 12p + 4n - 6$ gegeben. Für particuläre Lagen des Polygoncentrums kann auch eine Herabminderung dieser Zahl eintreten. Im ersten Falle sagen wir, P_0 habe den gewöhnlichen Typus, im letzteren Falle sprechen wir von Specialtypen.

Der geometrische Ort der Centren, deren Polygone Specialtypen zeigen, setzt sich aus einer unendlichen Menge von Stücken gerader Linien und gewisser Curven dritter Ordnung zusammen, welche eine neue Einteilung in Bereiche liefern, die ich allgemein durch Q bezeichne. Das Netz der Bereiche Q geht gleichfalls durch alle Substitutionen von Γ in sich selbst über. Der einzelne Bereich Q enthält nie zwei bezüglich Γ äquivalente Punkte. Es giebt nur eine endliche Anzahl inäquivalenter Bereiche Q, etwa m, sofern wir uns auf Gruppen mit endlichen p und n beschränken.

Irgend m inäquivalente Bereiche Q, welche einen zusammenhängenden Complex darstellen, liefern einen D. B. von Γ, den ich als einen natürlichen D. B. bezeichne. Derselbe lässt sich nur auf eine endliche Anzahl von Arten auswählen. Der Vorzug des natürlichen D. B. besteht darin, dass seine Randcurven aus Linien bestehen, welche mit der Gruppe Γ auf Grund einer organischen Gesetzmässigkeit eindeutig gegeben sind.

Die kanonischen D. B. entsprechen mit dem Verlauf ihrer Randcurven den bekannten kanonischen Querschnittsystemen geschlossener Flächen. Hier ist das Haupttheorem, dass sich der kanonische D. B. als geradliniges Polygon mit lauter concaven Winkeln fixiren lässt. Das Beweisverfahren dieses Satzes besteht in seinen einzelnen Schritten aus durchsichtigen geometrischen Schlüssen, wobei schliesslich das sogenannte Princip der Gruppencomposition eine Rolle spielt. Doch handelt es sich hierbei um eine so lange Kette von Schlüssen, dass eine Darstellung des fraglichen Nachweises hier ausgeschlossen ist.

Das angedeutete Theorem verhilft dazu, den Ueberblick über die Gesamtmannigfaltigkeit aller Gruppen mit endlichen Zahlen p, n zu gewinnen. Alle Gruppen, welche in p und n übereinstimmen, mögen eine „Gattung" von Gruppen bilden; (p, n) heisse der „Charakter" der Gattung. Alle Gruppen dieser Gattung mit $\nu \leqq n$ elliptischen Ecken, deren Winkel in irgend einer Folge $\frac{2\pi}{l_1}, \frac{2\pi}{l_2}, \ldots, \frac{2\pi}{l_\nu}$ sind, mögen eine in der Gattung enthaltene „Familie" von Gruppen darstellen; $(p, n; l_1, l_2, \ldots, l_\nu)$ heisse die „Signatur" der Familie. Es gilt das Theorem: Die sämtlichen Gruppen einer einzelnen Familie bilden ein Continuum von $(3n - \nu + 6p - 6)$ Dimensionen.

Dieses Continuum kann man analytisch mit den „Moduln der Gruppe" beherrschen. Man hat diese Moduln als Invarianten der von einem kanonischen Polygon gelieferten Gruppenerzeugenden zu fixiren. Polygone und Gruppen, die in einander transformirbar sind und also in diesem Sinne zu der gleichen „Klasse" gehören, haben dann immer dieselben

Moduln. Die letzteren lassen sich so bestimmen, dass sie die Klasse eindeutig definiren. Die Moduln sind reelle, aber nicht völlig willkürliche Variabele; vielmehr sind sie an gewisse „charakteristische Ungleichungen" gebunden, deren vollständige Aufstellung eine Hauptaufgabe der Theorie war. Die Angabe dieser Ungleichungen verbietet sich hier aus Raummangel.

Zur Theorie der gewöhnlichen Kettenbrüche.

Von

Felix Klein (Göttingen).

Sei $\omega = \frac{x}{y}$ eine reelle Grösse, die wir des bestimmteren Ausdrucks halber als irrational und positiv voraussetzen; mit $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots$ bezeichnen wir in üblicher Weise die unendlich vielen auf einander folgenden Näherungsbrüche der zugehörigen Kettenbruchentwickelung. Die ganzzahligen Punkte $x = p_\nu$, $y = q_\nu$ $(\nu = 1, 2, \ldots)$ liegen dann bekanntlich abwechselnd auf den beiden Seiten der geraden Linie $x - \omega y = 0$; man wird die Aufgabe stellen, das geometrische Gesetz dieser Näherungspunkte in möglichst einfacher Weise zu beschreiben. Im Gegensatze zu anderen Autoren beschränkte sich der Vortragende zu dem Zwecke auf die eine Hälfte der Näherungspunkte, etwa diejenigen mit ungeradem Index, also die Näherungspunkte, welche zwischen der Geraden ω und der positiven X-Axe eingeschlossen sind. Man betrachte die sämtlichen ganzzahligen Punkte, welche in dem genannten Sector oder auch auf der positiven X-Axe selbst liegen, befestige in jedem derselben einen kleinen Stift und schlinge um das Ganze einen Faden. Man erhält dann, was man das *geradlinige Umrisspolygon* der genannten Gitterpunkte nennen kann, und die Betrachtung zeigt, *dass die Näherungspunkte* $(p_1, q_1), (p_3, q_3), \ldots$ *nichts anderes sind als die Ecken dieses Umrisspolygons.*

Der Vortragende entwickelte weiter, wie man die so gefundene Interpretation der Näherungspunkte in der Theorie der binären indefiniten quadratischen Formen $f = ax^2 + bxy + cy^2$ benutzen kann. Sind ω', ω'' die beiden (reellen) Wurzeln, welche die Gleichung $f = 0$ für $\frac{x}{y}$ ergiebt, und die wir als irrational voraussetzen wollen, so construire man die

beiden geraden Linien $\frac{x}{y} = \omega'$ und $\frac{x}{y} = \omega''$ und wähle unter den 4 Sectoren, in welche dieselben die Ebene zerlegen, einen aus. In demselben liegen unendlich viele Gitterpunkte, d. h. Punkte mit ganzzahligen x, y. Wir schliessen dieselben wieder mit einem Faden ein und erhalten so, was wir das zugehörige (geradlinige) Umrisspolygon nennen können. Vortragender deutete nun an, wie man die ganze Lehre von der Reduction der Formen f an diesem Polygon geometrisch entwickeln kann, wobei gewisse Beziehungen sehr viel unmittelbarer hervortreten, als bei der gewöhnlichen, rein arithmetischen Darstellung.

So weit handelte es sich nur um neue Formulirung bereits bekannter Resultate. Aber diese Formulirungen übertragen sich von selbst auf höhere, z. B. ternäre Formen, wo sie dann auch ihrem Inhalte nach Neues enthalten. Man nehme z. B. eine cubische ternäre Form F(x, y, z), welche in das Product dreier reeller Linearfactoren zerfällt, die wir als irrational voraussetzen wollen. Gleich Null gesetzt, stellt dieselbe im gewöhnlichen System rechtwinkliger Parallelcoordinaten x, y, z drei Ebenen dar, die den Raum in acht Octanten zerlegen. Man wähle einen dieser Octanten und construire das ebenflächige Umrisspolyeder der in ihm enthaltenen ganzzahligen Punkte. Aus der Betrachtung dieser Umrisspolyeder folgt dann eine neue arithmetische Behandlung der Formen F (in Richtung des Reductions- bez. Aequivalenzproblems). Die Einzelheiten dieses Ansatzes hat Herr Furtwängler in seiner demnächst erscheinenden Göttinger Dissertation ausgeführt. — Oder man betrachte eine ternäre indefinite quadratische Form $\Phi(x, y, z)$. Hier giebt $\Phi = 0$ einen Kegel, und wir wollen der einfacheren Ausdrucksweise halber voraussetzen, dass $\Phi = 0$ auf seiner Oberfläche keine ganzzahligen Punkte enthalte. Wir nehmen dann die ganzzahligen Punkte, welche im Inneren der einen Kegelhälfte eingeschlossen sind, und construiren das zugehörige ebenflächige Umrisspolyeder. Wir erhalten von da eine Behandlung des Reductionsproblems der Formen Φ, welche mit elementareren Mitteln arbeitet, als die von Selling gegebene. Diese Theorie soll in die allgemeine Darstellung der Theorie der automorphen Functionen einer Variabelen eingearbeitet werden, welche der Vortragende zusammen mit Herrn Fricke vorbereitet.

Der Pascal'sche Satz.

Von

P. Gordan (Erlangen).

Der Pascal'sche Satz ist nun schon seit Jahrhunderten von allen Seiten beleuchtet worden, so dass es scheint, als ob nichts Neues hinzugefügt werden könnte. Wenn ich ihn trotzdem zum Thema meines Vortrags wählte, so leitete mich dabei die Absicht, an der Hand des Beweises Methoden zu erklären, welche auch bei der Untersuchung höherer Curven verwertet werden können. Was die Kegelschnitte selbst anbetrifft, so sind die Operationen bereits von vielen Autoren, ich nenne unter anderen Rosanes, angewandt worden.

Sechs Punkte auf einem Kegelschnitte.

Ehe ich an meine eigentliche Aufgabe herantrete, ist es notwendig, eine Vorfrage zu beantworten, nämlich die Bedingung dafür aufzustellen, dass 6 Punkte

$$X_{K1},\quad X_{K2},\quad X_{K3}\qquad (K = 1, 2, \ldots, 6)$$

auf einem Kegelschnitt liegen.

Es giebt 2 verschiedene Wege, diese Aufgabe zu lösen.

Der eine Weg besteht in der Aufstellung einer Determinante U mit den Zeilen

$$U = \left| X_{K1}^2 \quad X_{K1}X_{K2} \quad X_{K1}X_{K3} \quad X_{K2}^2 \quad X_{K2}X_{K3} \quad X_{K3}^2 \right|;$$

ihr Verschwinden giebt die gesuchte Bedingung.

Der andere Weg ist etwas umständlicher und setzt eine geometrische Construction voraus. Man verbinde 4 der 6 Punkte, etwa

$$1 \quad 2 \quad 3 \quad 4,$$

durch gerade Linien und combinire je zwei entsprechende Geraden zu uneigentlichen Kegelschnitten. In dieser Weise gelangt man zu dem Kegelschnittbüschel

$$(12X)(34X) + \lambda (13X)(24X).$$

Ihm gehört der Kegelschnitt an, auf dem die 6 Punkte liegen. Hieraus ergeben sich die Relationen

$$(125)(345) + \lambda (135)(245) = 0,$$
$$(126)(346) + \lambda (136)(246) = 0.$$

Eliminirt man λ, so erhält man den Ausdruck

$$V = (125)(345)(136)(246) - (126)(346)(135)(245),$$

dessen Verschwinden gleichfalls die gesuchte Bedingung ergiebt.

Die Identität $U = cV$.

Da sowohl

$$U = 0 \text{ als auch } V = 0$$

die Bedingung liefern, dass 6 Punkte auf einem Kegelschnitte liegen, so muss die Identität stattfinden

$$(1.) \qquad U = cV,$$

in welcher c numerisch ist.

Unsere eigentliche Aufgabe besteht darin, dieselbe direct zu beweisen.

Unterwirft man die 6 Punkte allen 6! Permutationen, so bleibt U bis auf das Vorzeichen unverändert, während V 6! Werte:

$$V_1, V_2, \ldots\ldots$$

annimmt. Da die Gleichung (1.) hierbei bestehen bleiben soll, so können sich diese Werte nur durch ihr Vorzeichen unterscheiden.

Um dies direct einzusehen, greife man 2 Werte V_i und V_k heraus, welche dadurch in einander übergehen, dass man 2 der 6 Punkte, etwa die Punkte 1 und 2, mit einander vertauscht. Die Rechnung liefert dann unmittelbar die Formel:

$$(2.) \qquad V_i + V_k = 0.$$

Die Identität $U = \Sigma c_i V_i$.

Da die V_ϱ bis auf das Vorzeichen übereinstimmen, so brauche ich nur zu zeigen, dass U ein Aggregat der V_ϱ ist:

$$(3.) \qquad U = \Sigma c_i V_\varrho.$$

Diese Identität bleibt bestehen, welche Werte auch die Coordinaten X_{ik} der 9 Punkte haben. Um die Formel anschaulicher zu machen, ersetze ich dieselben durch die Symbole von 6 ternären quadratischen Formen

$$a_{ik}^2 = 0,$$

so dass die Zeilen von U nunmehr die Form haben:

$$U = \left| a_{K1}^2 \quad a_{K1}a_{K2} \quad a_{K1}a_{K3} \quad a_{K2}^2 \quad a_{K2}a_{K3} \quad a_{K3}^2 \right|.$$

Um die 6-reihige Determinante U in 3-reihige Determinanten aufzulösen, benutze ich den Satz von Laplace.

Ich kann hierbei auf zwei verschiedenen Wegen mein Ziel erreichen; entweder ich zerschneide U in die 3 ersten Colonnen und die 3 letzten Colonnen, oder ich zerschneide U in die 3 ersten Zeilen und die 3 letzten Zeilen.

Zerschneidung nach Colonnen.

Zunächst unterwerfe ich U einer linearen Coordinaten-Transformation, deren Coefficienten ich durch x, y, z bezeichne. Ich erhalte dann eine neue Determinante U_1, welche die Zeilen besitzt:

$$U_1 = \left| a_{Kx}^2 \quad a_{Kx}\, a_{Ky} \quad a_{Kx}\, a_{Kz} \quad a_{Ky}^2 \quad a_{Ky}\, a_{Kz} \quad a_{Kz}^2 \right|$$

und mit U durch die Relation verbunden ist.

$$(4.) \qquad U_1 = U(xyz)^4.$$

Die dreireihigen Unterdeterminanten der 3 ersten Colonnen haben Werte der Form:

$$(abc)\, a_x\, b_x\, c_x (xyz) = \Delta_x^3\ (xyz),$$

und die dreireihigen Unterdeterminanten der 3 letzten Colonnen haben Werte der Form:

$$(deu)\,(afu)\,(efu) = u_s^3,$$

welche ich die Jacobi'sche und die Hermite'sche Form nenne. Die u sind die Coordinaten der Verbindungslinie von y und z. Die Symbole

a b c d e f

bedeuten die der 6 Kegelschnitte in irgend einer Permutation.

Die Laplace'sche Zerlegung erzeugt die Formel

$$U u_x^3 = \Sigma \Delta_x^3\, u_s^3,$$

aus welcher nach bekannten Reihenentwickelungen die Formel sich ergiebt:

$$(5.) \qquad cU = \Sigma \Delta_s^3 = \Sigma (abc)\,(ade)\,(bdf)\,(cef).$$

Zerschneidung nach Zeilen.

Die dreireihigen Determinanten A der 3 ersten Zeilen von U sind Coefficienten von Elementar-Combinanten $\mathfrak{A}$ der 3 ersten Kegelschnitte, und die dreireihigen Determinanten B der 3 letzten Zeilen sind Coefficienten von Elementar-Combinanten $\mathfrak{B}$ der 3 letzten Kegelschnitte.

Nun sind Δ und s die 2 einzigen Combinanten von 3 Kegelschnitten. Ich bezeichne diese Formen durch Δ_1, s_1 für die 3 letzten Kegelschnitte.

Da U eine Invariante ist, so ist es ein Aggregat von Ueberschiebungen. Man hat daher die Formel

$$U = c_1\, \Delta_{s_1}^3 + c_2\, \Delta_{1,s}^3;$$

und wenn man die 3 ersten Zeilen mit den 3 letzten vertauscht:

$$-U = c_2\, \Delta_{s_1}^3 + c_1\, \Delta_{1,s}^3,$$

also

$$(6.) \qquad 2U = (c_1 - c_2)\,(\Delta_{s_1}^3 - \Delta_{1,s}^3).$$

Correlative Verwandtschaft in n Dimensionen.

Von

Hermann Schubert (Hamburg).

Die Methoden, welche Zeuthen und der Vortragende für die abzählende Geometrie in unserem vorstellbaren Raume geschaffen haben, wurden 1884 von dem letzteren n-dimensional gestaltet. Dadurch erschienen die Anzahlen, welche bis dahin einzeln und beziehungslos berechnet waren, als Functionen der Dimension n des zu Grunde gelegten Raumes und der Zahlen, welche angeben, wie oft jede der gegebenen Bedingungen erfüllt werden soll. Die bisherigen Erfolge in der n-dimensionalen abzählenden Geometrie beruhen im wesentlichen auf der vom Vortragenden angegebenen und dann von Pieri und anderen italienischen Mathematikern benutzten Bezeichnungsweise für die charakteristischen Lagebedingungen, die man einem linearen Raume p-ter Dimension auferlegen kann. Wenn man unter einer eine Zahl umschliessenden eckigen Klammer einen linearen Raum versteht, dessen Dimension diese Zahl ist, so kann jede solche Bedingung nämlich durch das Symbol

$$(a_0 a_1 a_2 \dots a_p)$$

dargestellt werden, was bedeuten soll, dass ein $[a_0]$, ein $[a_1]$ u. s. w. bis $[a_p]$ so gegeben sind, dass immer jeder $[a_i]$ in dem $[a_{i+1}]$ liegt, und dass dann der [p] mit jedem $[a_k]$ einen [k] gemeinsam haben soll. Hiernach bedeutet z. B.: (07) die Bedingung, dass ein Strahl in einem siebendimensionalen linearen Raume liegen und dabei durch einen darin gegebenen Punkt gehen soll, (134) die Bedingung, dass eine Ebene in einem vierdimensionalen linearen Raume liegen und dabei einen darinliegenden Strahl schneiden soll, (124) die Bedingung, dass eine Ebene in einem vierdimensionalen linearen Raume liegen und eine darin liegende Ebene in einem Strahle schneiden soll u. s. w. Diese Bedingungen hat der Vortragende charakteristisch genannt, weil sie und sie allein in die allgemeine Formel eintreten, die das Charakteristikenproblem aller linearen Räume lösen. (Hamburger Mitteil. von 1886.)

Mit Benutzung dieser Bezeichnung entwickelte der Vortragende im 45. Bande der Math. Ann. die Functionen, welche die Anzahlen für Räume zweiten Grades beliebiger Dimensionen ausdrücken. Genau parallel dieser Untersuchung geht die Untersuchung, welche an die Stelle des Raumes zweiten Grades zwei correlativ verwandte p-dimensionale

lineare Räume setzt, und welche demgemäss zu den Verallgemeinerungen der Zahlen führt, die Sturm, Hirst und der Vortragende für projective Punktreihen, correlative Ebenen u. s. w. gefunden haben. Während aber die Ergebnisse der früheren Untersuchung noch nicht studirte, aus Binomialcoefficienten zusammengesetzte Ausdrücke sind, so sind die Ergebnisse der neuen Untersuchung elegant gestaltete Determinanten der Binomialcoefficienten. Nur der einfachste Fall möge hier Platz finden.

Es bezeichne für eine correlative Verwandtschaft, die in dem zu Grunde gelegten [n] zwischen einem [p] und einem [p]′ besteht, das Zeichen μ_1 die Bedingung, dass zwei gegebene [n—1] den [p] und den [p]′ in je einem [p—1] schneiden, die sich conjugirt sind, d. h. so beschaffen, dass der Punkt, der dem im [p] entstandenen [p—1] im [p]′ correlativ entspricht, auf dem im [p]′ entstandenen [p—1] liegt. Wenn nun für den [p] die Lagebedingung

$$(a_0 a_1 \ldots a_p),$$

für den [p]′ die Lagebedingung

$$(a'_0 a'_1 a'_2 \ldots a'_p)$$

gegeben sind, und wenn ausserdem

$$(a_0 + a_1 + \cdots + a_p) + (a'_0 + a'_1 + \cdots + a'_p) + p$$

Bedingungen μ_1 gegeben sind, so giebt es bei gänzlicher Unabhängigkeit der gegebenen Bedingungen von einander immer eine endliche Anzahl von Paaren correlativ verwandter [p], die sie sämmtlich erfüllen; und diese endliche Anzahl wird stets durch die folgende Binomialcoefficienten-Determinante ausgedrückt:

$$\begin{vmatrix} (a_0 + a'_0)_{a_0} & \ldots & (a_0 + a'_p)_{a_0} \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ (a_p + a'_0)_{a_p} & \ldots & (a_p + a'_p)_{a_p} \end{vmatrix}$$

Beispielsweise ist (23) (23)′ $\mu_1^{11} = 4_2 . 6_3 - 5_2 . 5_3 = 6 . 20 - 10 . 10 = 20$. Dies heisst in Worten, dass in unserm Raume sich bei 11 Paaren von gegebenen Ebenen 20-mal zwei Strahlen so legen lassen, dass die 11 Schnittpunkte, welche die einen 11 Ebenen auf dem einen Strahl ausschneiden, den 11 Schnittpunkten projectiv sind, die auf dem anderen Strahl durch die anderen 11 Ebenen entstehen. Ein zweites Beispiel ist:

$$(123)(123)' \mu_1^{14} = 4,$$

weil die Determinante

$$\begin{vmatrix} 2_1 & 3_1 & 4_1 \\ 3_2 & 4_2 & 5_2 \\ 4_3 & 5_3 & 6_3 \end{vmatrix}$$

den Wert 4 hat.

Da die gesuchte Anzahl 1 sein muss, wenn der eine [p] fest gegeben ist, der andere gar keine Lagebedingung erfüllen soll, so muss die obige Determinante für $a_i = i$ und $a_k' = n - p - k$ immer den Wert 1 erhalten. Also hat

$$\begin{vmatrix} e_0 & \dots & (e+f)_0 \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot & \cdot \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot & \cdot \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot & \cdot \\ e_f & \dots & (e+f)_f \end{vmatrix},$$

unabhängig von e und f, immer den Wert 1, ein Resultat, das auch durch die fundamentalen Determinanten-Eigenschaften leicht bewiesen werden kann.

Ueber gewisse lineare Differentialgleichungen.

Von

A. Gutzmer (Berlin).

Es wurden diejenigen linearen Differentialgleichungen betrachtet, welche durch Iteration aus einer linearen Gleichung erster Ordnung, d. h. durch wiederholte Composition eines linearen Differentialausdrucks erster Ordnung mit sich selbst, entstehen, und über welche der Vortragende mehrere Notizen veröffentlicht hat. (Vgl. besonders: Sitzungsberichte der Böhm. Gesellschaft der Wissenschaften, 1892, und Journal für die reine und angewandte Mathematik, Bd. 115, 1895). Zunächst wurde nachgewiesen, dass alle linearen homogenen Differentialgleichungen, deren Integrale aus einem einzigen durch wiederholte Multiplication desselben mit einer und derselben Function der Unabhängigen entstehen, als Iterationen linearer homogener Gleichungen erster Ordnung dargestellt werden können.

Damit lässt sich dann in einfachster Weise der Satz gewinnen, dass jede lineare homogene Differentialgleichung zweiter Ordnung als Iteration einer solchen Gleichung erster Ordnung darstellbar ist, und ferner, dass

diejenigen linearen homogenen Gleichungen, denen die Potenzen des Integrals einer Gleichung zweiter Ordnung genügen, dieselbe Eigenschaft besitzen. Auch wurde die einfache Beziehung hergeleitet, welche zwischen den beiden Gleichungen erster Ordnung besteht, von denen die eine die Gleichung zweiter Ordnung, die andere diejenige Gleichung durch Iteration liefert, welcher die betrachtete Potenz des Integrals dieser Gleichung zweiter Ordnung genügt.

Zum Schluss wurde noch die Iteration nichthomogener linearer Differentialgleichungen behandelt; dies führt zu einer Klasse nichthomogener Gleichungen aller Ordnungen, deren Integrale niedergeschrieben werden können, und welche geeignet erscheinen, in Vorlesungen zur Demonstration der Integration nichthomogener linearer Differentialgleichungen zu dienen.

Ueber den Feuerbach'schen Kreis und die Steiner'sche Curve vierter Ordnung und dritter Klasse.

Von

W. Godt (Lübeck).

Die Ecken eines Dreiecks heissen $\mathrm{A}, \mathrm{B}, \Gamma$, die Mitten seiner Seiten A, B, C, die Fusspunkte seiner Höhen A^1, B^1, C^1. Die Punkte A, B, C, A^1, B^1, C^1 liegen dann in der Peripherie eines Kreises Φ, und dieser wird nach Feuerbach und Steiner von den vier Berührungskreisen des Dreiecks $\mathrm{AB}\Gamma$ berührt in vier Punkten R_0, R_1, R_2, R_3.

Die Diagonalecken des Vierecks $R_0 R_1 R_2 R_3$, sie heissen R_a, R_b, R_c, sind die Schnittpunkte entsprechender Seiten der Dreiecke ABC und $A^1B^1C^1$.

Die drei Paar Winkelhalbirenden von Dreieck ABC treffen die entsprechenden Seiten von Dreieck $R_aR_bR_c$ in drei Punktepaaren, und diese sind die Gegeneckenpaare des vollständigen Vierseits der Tangenten von Φ in R_0, R_1, R_2, R_3.

Auf Φ zeichnet sich noch ein zweites Viereck $Q_0 Q_1 Q_2 Q_3$ aus; seine Diagonalecken Q_a, Q_b, Q_c fallen auch in die Seiten von ABC.

Die Geraden $R_a A$, $R_b B$ und $R_c C$ gehen durch denselben Punkt Q^1 von Φ. Die Geraden $Q_a A$, $Q_b B$ und $Q_c C$ gehen durch denselben Punkt R^1 von Φ. Die Punkte Q^1 und R^1 stehen zu dem Dreiecke $\mathrm{A}^1\mathrm{B}^1\Gamma^1$, das seine Seitenmitten in A^1, B^1, C^1 hat, in derselben Beziehung wie etwa Q_0 und R_0 zum Dreieck $\mathrm{AB}\Gamma$.

Durch Q^1 geht der Kegelschnitt, der die Seiten von $AB\Gamma$ in A, B, C berührt. Durch R^1 geht der Kegelschnitt, der die Seiten von $AB\Gamma$ in A^1, B^1, C^1 berührt. Beide Kegelschnitte sind in anderem Zusammenhange wiederholt von Steiner betrachtet.

Wie Dreieck $AB\Gamma$ auf $A^1B^1\Gamma^1$ führt, so führt dieses auf $A^2B^2\Gamma^2$ und so fort, und rückwärts kann man jedes Dreieck aus vier verschiedenen vorangehenden abgeleitet denken. Nimmt man in jedem Dreieck noch die drei Höhenlinien hinzu, so erhält man lauter vollständige Vierecke. Die Seiten aller dieser Vierecke sind Strahlen eines und desselben Büschels dritter Klasse und vierter Ordnung, des Steiner'schen. Alle von Steiner angegebenen Eigenschaften desselben ergeben sich mit grösster Einfachheit und daneben manche andere interessante Beziehungen metrischer Art.

Die hier auftretenden Vierecke stehen in engster Beziehung zu einem linearen Gewebe von Kegelschnitten, das aus lauter gleichseitigen Hyperbeln besteht. Die Gleichung desselben tritt in einer sehr durchsichtigen Form auf, aus der eine Fülle von schönen Beziehungen zu den Dreiecken $AB\Gamma$ u. s. f. und ihren Berührungskreisen abzulesen ist.

Der Vortragende deutete zum Schlusse an, dass er seine Betrachtungen als Anwendung einer allgemeineren Methode auf einen metrisch ausgezeichneten besonderen Fall der cubischen binären Form ansieht, von deren Leistungsfähigkeit er hiermit einen Beweis vorzulegen wünsche.

Zur geometrischen Deutung der homogenen Coordinaten.

Von

G. Kohn (Wien.)

Die homogenen Coordinaten $x_1, x_2, \ldots x_{n+1}$ eines Punktes X im R_n lassen sich deuten:

1. als homogene Coordinaten des $(n+3)$-elementigen Wurfs, der auf der Verbindungslinie von X mit dem Einheitspunkte bestimmt wird von den Schnittpunkten der Coordinatenebenen im Verein mit dem Punkte X und dem Einheitspunkte;

2. als homogene Coordinaten des Wurfs, den die Ecken der Coordinatenpyramide im Verein mit dem Einheitspunkte und dem Punkte X bestimmen.

Dabei werden unter den homogenen Coordinaten von $n+3$ Elementen eines einförmigen Trägers die (in ihren Verhältnissen bestimmten) Parameter verstanden, die den $n+1$ ersten Elementen in einer Parameterverteilung zukommen, in welcher dem vorletzten Element der Parameter 0, dem letzten der Parameter ∞ zugehört. Unter dem Wurf von $n+3$ Punkten des R_n ist aber der Wurf verstanden, den diese Punkte auf der hindurchgehenden Normcurve bestimmen.

Ueber cubische Constructionen.

Von

Franz London (Breslau).

Jedes Constructionsproblem, welches die Auffindung nur eines einzigen unbekannten Elementes erfordert, lässt sich bekanntlich mit alleiniger Hülfe des Lineals ausführen. Bei Aufgaben, welche die Auffindung zweier unbekannter Elemente (z. B. eines Punktepaars) verlangen, hat man ausser dem Lineal noch den Zirkel zu Hülfe zu nehmen; dabei hat Steiner in seiner klassischen Abhandlung: „Ueber die geometrischen Constructionen, ausgeführt mittels der geraden Linie und eines festen Kreises" (1833) gezeigt, dass sich die Anwendung des Zirkels auf ein Minimum beschränken lasse, indem er bewies, dass alle quadratischen Constructionen mit alleiniger Hülfe des Lineals ausführbar werden, falls in der Zeichnungs-Ebene ein fester Kreis ein für alle Mal gezeichnet vorliegt. Für die Constructionen, bei welchen es sich um die Auffindung dreier unbekannter Elemente (z. B. dreier Punkte) handelt, die sogenannten cubischen Constructionen, wurde die Frage nach den zu ihrer Ausführung erforderlichen Hülfsmitteln im Jahre 1868 erledigt, gelegentlich der Bewerbung um den Steiner-Preis der Berliner Akademie. Es wurde in den beiden preisgekrönten Arbeiten von Herrn Kortum*) und Stephen Smith**) gezeigt, dass, falls ein fester Kegelschnitt (der aber kein Kreis sein darf) ein für alle Mal gezeichnet vorliegt, sich alle cubischen Constructionen mit alleiniger Hülfe von Zirkel und Lineal ausführen lassen. Es ist die Frage, ob diese von Smith

---

*) Kortum: Ueber geometrische Aufgaben dritten und vierten Grades, Bonn 1869.

**) Smith: Mémoire sur quelques problèmes cubiques et biquadratiques; Annali di matematica Ser. II, Tomo III.

und Kortum angegebenen Hülfsmittel für cubische Constructionen die einfachsten sind, und es liegt der Gedanke nahe, zu untersuchen, ob die Ausführung der cubischen Constructionen nicht auch mit alleiniger Hülfe des Lineals gelingt, falls eine feste Curve III. Ordnung, und zwar eine möglichst specielle und einfach herstellbare, ein für alle Mal gezeichnet vorliegt. Eine derartige Behandlung der cubischen Constructionen erscheint angemessener und einfacher als die bisherige; angemessener, weil dann eine völlige Analogie mit der Steiner'schen Behandlung quadratischer Aufgaben erreicht ist; einfacher, weil man nunmehr des Zirkels ganz entraten kann, wobei zwar an Stelle der festen Curve II. Ordnung eine feste Curve III. Ordnung tritt, diese aber speciell und so einfach gewählt werden kann, dass ihre Herstellung keine grössere Schwierigkeit verursacht, als die einer allgemeinen Curve II. Ordnung. Man kann in der That beweisen, dass sich jede cubische Construction mit den genannten Hülfsmitteln vollziehen lässt. Da durch die Methode von Smith-Kortum sich jede cubische Construction zurückführen lässt auf die Auffindung der 3 letzten Schnittpunkte x, y, z eines Kreises K mit einem festen Kegelschnitt C^2, wobei der vierte Schnittpunkt von K und C^2 bekannt ist, so wird es genügen, zu zeigen, dass sich das Punkttripel x, y, z mit alleiniger Hülfe des Lineals und einer festen Curve III. Ordnung C^3 auffinden lässt. Dies geschieht, indem man eine quadratische Verwandtschaft bestimmt, in welcher der Curve II. Ordnung C^2 die Curve III. Ordnung C^3, dem Kreise K eine Gerade G entspricht, und bei welcher zu jedem Punkte der entsprechende mit alleiniger Hülfe des Lineals gefunden wird. Ist diese Verwandtschaft gefunden, so construirt man die dem Kreise K entsprechende Gerade G, bestimmt ihre 3 Schnittpunkte mit C^3 — das ist die einzige erforderliche cubische Operation — und sucht diejenigen 3 Punkte, von welchen diese 3 Schnittpunkte in Bezug auf die quadratische Verwandtschaft die entsprechenden Punkte sind; diese sind die 3 gesuchten Schnittpunkte x, y, z, welche der Kreis K aus C^2 ausschneidet, sie sind mit alleiniger Hülfe des Lineals und der festen C^3 construirt, und da alle cubischen Constructionen auf die Bestimmung eines derartigen Punktetripels zurückkommen, so lässt sich somit jede cubische Aufgabe in der genannten Weise behandeln. Die feste Curve III. Ordnung C^3 muss einen Doppelpunkt besitzen, da sie in der obigen quadratischen Verwandtschaft der Curve II. Ordnung C^2 entspricht, also wie diese rational ist. Es ergiebt sich somit: Ist eine rationale Curve III. Ordnung ein für alle Mal gezeichnet, so lässt sich jede cubische Construction

mit alleiniger Hülfe des Lineals ausführen. Die ein für alle Mal gezeichnete C^3 wird man möglichst einfach wählen; erteilt man derselben einen Rückkehrpunkt, so wird sich die obige quadratische Verwandtschaft, auf deren Herstellung alles ankommt, besonders einfach herstellen lassen. Ferner wird man passend den einen unendlich fernen Punkt mit dem Inflexionspunkt, die beiden anderen mit den beiden unendlich fernen Kreispunkten zusammenfallen lassen. Dadurch erhält einerseits C^3 eine Symmetrie-Axe, andererseits wird die absolute Involution linear construirbar, so dass man auch metrische Constructionsaufgaben in der genannten Art nunmehr behandeln kann. Die so entstehende C^3 wird eine Cissoide, die man sowohl durch sehr leichte Constructionen punktweise herstellen, als auch durch einen sehr einfachen, schon von Newton angegebenen Mechanismus in einem Zuge zeichnen kann.

Ueber unendliche Reihen und Producte.

Von

L. Schendel (Berlin).

(Die Arbeit wurde von Herrn Fr. Meyer vorgelegt).

Ueber eine gewisse Einhüllende.

Von

P. H. Schoute (Groningen).

(Die Arbeit wurde von Herrn A. Gutzmer vorgelegt).

Ueber eine verwandte Gruppe thermodynamischer, elektrodynamischer und astrophysikalischer Thatsachen.

Von

J. R. Schütz (Göttingen).

1. Es ist eine auf Galilei zurückgehende Anschauung, dass der Luftdruck, den ein wagerechtes Flächenstück in der freien unbewegten

Lufthülle der Erde erfährt, genau gleich dem Gewichte der über diesem Flächenstück senkrecht lagernden Luftsäule ist.

Diese Anschauung, durch die barometrischen Versuche Torricelli's verdeutlicht, ist zu einer reichen Quelle von Natur-Erkenntnissen geworden, ja eine neue blühende Wissenschaft, die Meteorologie, ist wesentlich ihr entsprungen. Nichtsdestoweniger ist sie durch keinerlei Erfahrung bewiesen, und man kann ihr die folgende Gegenansicht zunächst als gleichberechtigt gegenüberstellen:

Der Druck der freien unbewegten Lufthülle auf ein wagerechtes Flächenstück ist nicht genau gleich dem Gewichte der über demselben senkrecht lagernden Luftsäule, sondern gleich diesem Gewichte, vermehrt um eine Constante k.

Uebrigens ist diese Gegenansicht sogar vorzugsberechtigt; ihr Beweis und zugleich die Berechnung der Constanten k fliesst aus folgender Ueberlegung: Im Sinne der gewöhnlichen barometrischen Höhenformel muss der Luftdruck mit stetig wachsender Entfernung H vom Erdmittelpunkte allerdings verschwinden, und zwar von der Ordnung der Function $\frac{1}{e^H}$; aber hierbei ist die Abnahme der Erdschwere mit wachsender Höhe vernachlässigt; nach der strengen Formel muss der Luftdruck von der Ordnung der Function $ke^{\frac{1}{H}}$ abnehmen; diese Function ist der obigen sehr ähnlich gebaut; aber sie nähert sich mit stetig wachsendem H nicht unbegrenzt der Null, sondern dem endlichen, angebbaren Grenzwerte k.

Diese Ueberlegung, für jeden einzelnen Himmelskörper sowohl, als für die Gesamtheit aller durchgeführt, ergiebt das Postulat:

Der Weltenraum ist von ponderabelen Gasen erfüllt, deren Druck nirgendwo, also auch dort nicht, wo der Gravitationseinfluss der Gestirne verschwindet, unter einen endlichen Grenzwert sinkt. Die unendliche Gesamtheit der den Weltenraum erfüllenden ponderabelen Gase soll der kosmische Gaskörper, der besondere Grenzwert k soll der kosmische Gasdruck im Anziehungsbereiche der Erde genannt sein.

2. Aus dieser Anschauung entspringt der theoretischen Physik folgendes Problem: Die möglichen thermischen, mechanischen, thermodynamischen und ponderomotorischen Gleichgewichtszustände für heterogene Systeme aufzusuchen, auf welche äussere Kräfte wirken.

Wesentlich dasselbe Problem ist zugleich grundlegend für eine Elektrodynamik, welche die Forderung*) erhebt, dass der Zustand des Aethers nicht schon durch einen einzigen (mechanischen) Parameter, sondern erst durch zwei Parameter (einen mechanischen und einen von dem Wesen eines thermischen) zureichend bestimmbar ist; und welche dem entsprechend auch auf die Forderung der absoluten Incompressibilität des Aethers verzichtet.

Des Vortragenden Untersuchungen wurzeln in einer so definirten Elektrodynamik. Einzelne Ergebnisse derselben scheinen sich aber im Makrokosmos der Gestirne wiederzuspiegeln; wegen ihrer grösseren Anschaulichkeit sollen einige dieser letzteren hier Platz finden.

3. Vorerst wird die Erwägung hingestellt, ob es auch noch einen guten physikalischen Sinn hat, den Grenzwert k für den Luftdruck einzuführen. Ein solches Bedenken ist freilich überflüssig, wenn man sich auf den Standpunkt einer von jeglicher bildlichen Vorstellung losgelösten Thermodynamik stellt; denn daselbst erscheinen Druck und Temperatur als starre Coordinaten, und man hat keinen zureichenden Grund, bei irgend einem Zahlenwerte derselben Halt zu machen. Hier zeigt sich die Notwendigkeit einer gastheoretischen Ueberwachung thermodynamischer Erwägungen. Welchen Sinn hätte es noch, von Druck, welchen Sinn zumal, von Temperatur zu sprechen, wenn vielleicht in einer Cubikmeile oder gar in Sternenweiten $1\frac{1}{2}$ Gasmolecüle wimmeln? Welchen Sinn, hier noch eine Differentialgleichung anzusetzen?

Nur um ein bestimmtes Zahlenbeispiel für den Grenzwert k zu erhalten, werde willkürlich angenommen, es sei die Temperatur des kosmischen Gaskörpers allenthalben gleichmässig, und zwar gleich jener des schmelzenden Eises; ferner gelte das Mariotte'sche Gesetz bis zu den grössten Verdünnungen; auch herrsche Diffusionsgleichgewicht. Dann lässt sich der Grenzwert k, bezogen auf eine bestimmte Gasart der Luft, in der bequemen Form darstellen

$$k = n^{-\frac{R}{A}},$$

worin als Druckeinheit der Partialdruck des betreffenden Gases an einer

*) Dass zugleich mit dieser Forderung eine stufenförmige Erweiterung des zweiten Hauptsatzes der Thermodynamik platzgreift, mit welcher das Entropiegesetz nicht mehr streng verträglich ist, hat der V. in der zu Lübeck gepflogenen Debatte über die Grundlagen der Energielehre hervorgehoben.

beliebigen Stelle der Atmosphäre, für R die Entfernung dieser Stelle vom Erdmittelpunkte, für A die verticale Erhebung, innerhalb deren der Partialdruck auf den nten Teil seines Wertes sinkt, endlich für n irgend eine beliebige Zahl (grösser als 1) zu wählen ist.

Es seien nunmehr aus der Luft alle Gase entfernt gedacht mit Ausnahme des Wasserstoffs. Man darf annehmen, dass alsdann der Druck an der Erdoberfläche nur den 10 000. Teil einer Atmosphäre beträgt (Boussingault). Für k erhält man hieraus den Druck von 10^{-28} Atmosphären. Dieser bedeutet, dass unter den genannten Voraussetzungen und selbst, wenn die Erde allein, ausser ihr kein Gestirn, kein Meteor und kein kosmisches Staubteilchen im Weltenraume vorhanden wäre, auf eine Cubikmeile Weltenraumes allenthalben mehr als rund zehn Milliarden Wasserstoffmolecüle zu zählen sind. (Dieselbe Rechnung, für den an der Erdoberfläche 100000mal dichteren Stickstoff der Luft durchgeführt, ergiebt, dass ebensoviele Stickstoffmolecüle erst in einem Raume zu erwarten sind, zu dessen Durchquerung das Licht 10^{258} Jahre braucht.)

3. In den kosmischen Gaskörper werden gravitirende Kugeln von den Massen- und Grössendimensionen der Himmelskörper getaucht. Es wird von atmosphärischen Ladungen der Himmelskörper gesprochen; diese Ladungen bedingen scheinbare ponderomotorische Kräfte, welche sich über die Gravitationskräfte überlagern; wegen ihrer Kleinheit kommen diese Kräfte nicht in Betracht; doch ist bemerkenswert, dass sie nur durch eine analytische, nicht schon durch eine algebraische Formel exact beschrieben werden können.

Von allgemeinem mechanischen Interesse möchte folgende Erwägung sein: Man kann die atmosphärischen Ladungen der Himmelskörper als Zwangszustände des kosmischen Gaskörpers auffassen; der Zwang ist ein innerer, weil durch die gravitirenden Kräfte des Systems bedingt; wären aber dieselben Zwangszustände dem (für den Augenblick als imponderabel vorgestellten) kosmischen Gaskörper eingeprägt, so würden neue scheinbare ponderomotorische Kräfte höchst beträchtlicher Grössenordnung ins Spiel treten. Die Untersuchung solcher und ähnlich definirter eingeprägter Zwangszustände ungeordneter Bewegungen ist — übertragen auf den Mikrokosmos der Atome — einer vorurteilslosen Auffassung des Begriffes der ponderabelen Materie sehr förderlich*).

---

*) Es sei an dieser Stelle gestattet, wenigstens ein einziges Beispiel in analytischer Schärfe hinzustellen: Ein imponderabeles Medium sei mit

4. Die soeben hingestellten Betrachtungen haben schon deshalb vorläufig keine nennenswerte praktische Bedeutung, weil sie nur für ruhende (rotations- und revolutionslose) Himmelskörper gelten. Sind Rotationen und Revolutionen vorhanden, dann treten neue Erscheinungsformen, zumal auch neue ponderomotorische Kräfte auf, und die Gleichungen, durch welche sich alsdann der mechanische Zustand des kosmischen Gaskörpers in Entfernungen von den Himmelskörpern, welche gross sind gegen deren Radien, zureichend beschreiben lässt, stehen mit den Maxwell'schen Gleichungen des elektromagnetischen Feldes in Uebereinstimmung.

---

einer verborgenen Bewegungsform ausgestattet, ganz von der Art der ungeordneten und demzufolge verborgenen inneren Bewegung, welche die kinetische Gastheorie der groben Materie zugedacht hat. Die gesamte im Volumelemente dv_1 verborgene Bewegungsenergie sei mit $E dv_1$ bezeichnet. Es ist nothwendig und zureichend, diese zwei Postulate voranzustellen:

a) E, als eindeutige Function des Raumes aufgefasst, ändere sich darin nach der analytischen Stetigkeit;

b) die ungleichmässige Verteilung der Bewegungsenergie im Raume sei an eingeprägte Zwangszustände gebunden.

Willkürlich werde als Mass M_1 des Bewegungszwanges in einem vorgegebenen Bereiche das über dasselbe erstreckte Integral

$$M_1 = -\frac{1}{4\pi}\int\left(\frac{\partial^2 Q}{\partial x^2} + \frac{\partial^2 Q}{\partial y^2} + \frac{\partial^2 Q}{\partial z^2}\right) dv_1$$

festgesetzt, worin die Function Q durch die partielle Differentialgleichung erster Ordnung $\left(\frac{\partial Q}{\partial x}\right)^2 + \left(\frac{\partial Q}{\partial y}\right)^2 + \left(\frac{\partial Q}{\partial z}\right)^2 = E(x, y, z)$, sowie durch analytische Nebenbedingungen definirt ist. [Wegen des Postulates a) existirt immer eine und nur eine analytische Function, welche in dem vorgegebenen Bereiche mit Q identisch ist.] Alsdann fliesst aus dem Princip der geradesten Bahn der Satz: dass zwei beliebig vorgegebene Bereiche aufeinander scheinbare ponderomotorische Kräfte ausüben, welche in jedem Augenblicke genau durch das Newton'sche Kraftgesetz $\iint \frac{M_1 M_2}{r_{12}^2} dv_1 dv_2$ beschrieben sind; worin M_1 und M_2 die Masszahlen für den Bewegungszwang in den beiden Volumelementen dv_1 und dv_2, r_{12} die Entfernung derselben bedeutet, und die Integrationen über beide Bereiche zu erstrecken sind. (Es scheint nicht völlig unwahrscheinlich, dass v. Helmholtz — unter dem frischen Eindrucke der Durchsicht der Correcturbogen zum Hertz'schen Werke über das Princip der geradesten Bahn — solcherlei Beispiele im Sinne hatte, als er die leider nicht mehr publicirte Wiener Mitteilung „Ueber verborgene Bewegungen und scheinbare Substanzen" ankündigte.)

5. Dies ist offenbar auch ein wesentlicher Unterschied des hier zu Grunde gelegten Postulates gegen die Galilei'sche These: dass nach dieser letzteren die Erde und vielleicht auch die übrigen Himmelskörper endliche Luftvorräte besitzen und mit denselben jahraus jahrein einen von kosmischen Einflüssen nur mittelbar berührten Haushalt führen; während nach dem ersteren keinem der Himmelskörper ein fester Vorrat atmosphärischen Besitzes zukommt, sondern der Kosmos selbst der unendliche und unerschöpfliche Vorratsspeicher hierfür ist, und die sogenannten Atmosphären der Himmelskörper nichts anderes vorstellen, als die Aeusserungen von Gleichgewichtszuständen des kosmischen Gaskörpers. Hier wird die Meteorologie zu einer Randwertaufgabe. Es kann sich nicht der Zustand des kosmischen Gaskörpers an der Oberfläche eines beliebigen Himmelskörpers ändern, ohne mit Notwendigkeit Aenderungen an den Oberflächen aller übrigen Himmelskörper nach sich zu ziehen.

Der Vortragende postulirt den idealen Fall, dass die Oberflächenbedingungen der Sonne periodisch unabhängig veränderlich sind, und dass dies in der Periode der Sonnenflecken seinen sichtbaren Ausdruck findet. Eine gleichzählige Periode müssen die Zustandsschwankungen des kosmischen Gaskörpers im Bereiche des ganzen Sonnensystems, und eine gleichzählige Periode demnach auch die meteorologischen Randwerte an der Oberfläche jedes einzelnen Planeten zeigen.

Aber man erkennt, dass aus dieser Anschauung die Forderung fliesst: dass diese Periodengänge gegen einander im allgemeinen beträchtliche Phasenverschiebungen aufweisen müssten. Dieser Forderung wird durch die meteorologische Erfahrung so wenig widersprochen, dass sogar gewissermaassen die Existenz dieser Phasenverschiebungen sicherer beglaubigt ist als die Existenz der Perioden selbst*).

Die Phasenverschiebungen der Perioden jener meteorologischen Elemente, welche durch mechanische Zustandsänderungen des kosmischen Gaskörpers übertragen werden, lassen sich übrigens dazu verwerten, die Temperatur des Weltraumes der Grössenordnung nach zu bestimmen. Bedeutet π die Periode der Sonnenflecken, φ die

*) Erk, Vortrag auf der Wiener Naturforscherversammlung. Eine sehr gründliche Zusammenstellung des einschlägigen Materials hat van Bebber gegeben; Handbuch der ausübenden Witterungskunde, Stuttgart 1885, I, pag. 199 bis 259; insbesondere Seite 258.

Phasenverschiebung, beide ausgedrückt in Jahren, σ das mittlere Moleculargewicht des kosmischen Gaskörpers (welches hier wohl gleich 2 gesetzt werden darf), E den Radius der Ekliptik, ausgedrückt in geographischen Meilen, so ist die gesuchte mittlere Temperatur T des kosmischen Gaskörpers, im Bereiche der Ekliptik, durch die Formel gegeben

$$T = 5 \,.\, 10^{-10} \,.\, \sigma \left(\frac{E}{\varphi + \frac{1}{2} n \pi} \right)^2,$$

ausgedrückt in absoluten Celsiusgraden; n ist eine, jedenfalls kleine, ganze Zahl (die Null nicht ausgeschlossen), welche durch eine sorgfältige Feststellung und Vergleichung der Periodengänge ein für allemal zu bestimmen ist; sie bedeutet offenbar die Anzahl der Verschiebungen um eine halbe Periode. Es braucht kaum bemerkt zu werden, dass die meteorologischen Randwerte hier zweckmässig als Mittelwerte, genommen über die ganze Erdoberfläche, zu verstehen sind.

6. Es ist schon eingangs erwähnt worden und möchte hier nochmals betont sein, dass das hier hingestellte Problem sein eigentlichstes Interesse erst gewinnt, wenn man den kosmischen Gaskörper als heterogenes thermodynamisches System auffasst und den darin eingebetteten kosmischen Staub, die Meteore und die Himmelskörper als thermodynamische Niederschläge desselben, hergestellt in Zeitläuften von Aeonen, und formenreich gestaltet durch ponderomotorische Anziehungen und etwaige Zertrümmerungen.

Als erstes bemerkenswertes allgemeineres Ergebniss der Theorie eines solchen Systems ist die Erkenntniss hinzustellen, dass alsdann stabile Gleichgewichtszustände nicht nur nicht erreichbar, sondern überhaupt — auch rein analytisch betrachtet — gar nicht möglich sind. Hier erwächst der theoretischen Naturbeschreibung zum ersten Male unabweisbar der Zwang, sich ihres gewohnten scharfen Zieles, Bedingungen von Gleichgewichtszuständen aufzusuchen, zu begeben und in die weit verwickeltere Untersuchung der Bedingungen des Wettstreites idealer Gleichgewichtszustände einzutreten.

Diffractionsprobleme in exacter Behandlung.

Von

A. Sommerfeld (Göttingen).

Unter den verschiedenen physikalischen Disciplinen scheint die Optik in mathematischer Hinsicht eine isolirte Stellung einzunehmen. Während nämlich im allgemeinen die physikalischen Probleme zu schwierigen Randwertaufgaben Anlass geben, machen wir uns die Verteilung von Licht und Schatten auf Grund weniger primitiver Gesetze: der geradlinigen Fortpflanzung der Lichtstrahlen etc., klar. Dieses Verfahren entspricht genau dem Standpunkte der älteren Emissionstheorie. Es entsteht die Frage: Ist es auch vom Standpunkte der heutigen Theorie zu rechtfertigen? Sind die so gefundenen Lösungen wirkliche Lösungen der optischen Differentialgleichungen? Die Antwort lautet: Nein, es sind nur Grenzfälle von exacten Lösungen für den Fall, dass die Wellenlänge (λ) des Lichtes gleich Null gesetzt wird. Allerdings kommen sie den wirklichen Lösungen sehr nahe, man möchte sagen: glücklicher Weise; denn nur darauf beruht es, dass wir uns mit Hülfe des Auges in der Aussenwelt orientiren können, ohne mathematische Betrachtungen anstellen zu brauchen.

Diejenigen Erscheinungen, bei denen die Abweichung der exacten Lösungen von jenen emissiven besonders merklich wird, nennt man Beugungserscheinungen. Merkwürdiger Weise gelingt es, vom Boden der gewöhnlichen Optik aus auch diesen annähernd gerecht zu werden durch eine Anwendung des Huygens'schen Principes. Dasselbe gestattet, eine Lösung u der optischen Differentialgleichungen für das Innere eines Gebietes anzugeben, wenn auf der Oberfläche u und $\frac{\partial u}{\partial n}$ bekannt sind. Letzteres ist leider bei den beabsichtigten Anwendungen keineswegs der Fall. Man hilft sich damit, dass man als Oberflächenwerte in die Formel des Huygens'schen Principes solche Werte einträgt, die sich im Falle $\lambda = 0$ ergeben würden. Natürlich kommt man so zu keiner exacten Beschreibung der Beugungserscheinungen, sondern wieder nur zu einer angenäherten, und auch dieses nur unter gewissen Umständen.

Darauf wird gezeigt, dass die exacte Behandlung der einfachsten Beugungsprobleme auf mehrwertige Functionen führt. Der fremde Körper sei ein ebener, unendlich dünner Schirm, welcher als vollkommener

Leiter der Elektricität vorausgesetzt wird. Irgendwo im Raume befinde sich ein leuchtender Punkt P. Der optische Zustand lässt sich durch eine Funktion u charakterisiren, welche folgenden Bedingungen zu genügen hat: 1) u erfüllt die Differentialgleichung $\Delta u + k^2 u = 0$ im ganzen Raume ($k = \frac{2\pi}{\lambda}$ ist eine Constante), 2) u verschwindet in Punkten des Schirmes, 3) u wird unendlich im leuchtenden Punkte P, und nur in diesem.

Eine so einfache Oberflächenbedingung wie 2) wird man nach dem Spiegelungsprincipe zu erfüllen suchen. Spiegelt man aber P in Bezug auf die Ebene des Schirmes, so entsteht eine zweite Unendlichkeitsstelle der Function, während die Bedingung 3) uns verbietet, eine solche irgendwo zu schaffen. In dem gewöhnlichen Raume ist also für den Spiegelungsprocess kein Platz. Deshalb gehen wir in einen Riemann-schen Doppelraum; wir denken uns also in den gewöhnlichen realen Raum einen zweiten hypothetischen hineingeschoben, welcher mit dem ersten längs der Ebene des Schirmes zusammenhängt. Der Schirmrand ist Verzweigungscurve. Nun denken wir eine Function U hergestellt, welche 1) in dem Doppelraum eindeutig ist, 2) der Gleichung $\Delta U + k^2 U = 0$ genügt, 3) in dem einen Punkte P unendlich wird. Sie heisse U(P). Es sei $\overline{P}$ der Spiegelpunkt von P, welcher jetzt in das hypothetische Raumexemplar fällt. Wir denken uns in derselben Weise eine Function $U(\overline{P})$ hergestellt, welche in $\overline{P}$ unendlich wird. Dann genügt

$$u = U(P) - U(\overline{P})$$

den sämtlichen Bedingungen des Beugungsproblemes. Es kommt also Alles darauf an, Lösungen der genannten Differentialgleichung zu finden, welche in einem Riemann'schen Raume eindeutig sind.

Mathematisch interessanter wird die Frage, wenn man sie weiter specialisirt, wenn man nämlich nur nach solchen Lösungen fragt, die von einer Coordinate (z) unabhängig sind. Dann kann man die Betrachtung auf die xy-Ebene beschränken; von dem Riemann'schen Raum kommt nur sein Schnitt mit dieser Ebene in Betracht, welcher eine Riemann'sche Fläche im gewöhnlichen Sinne wird. Die Aufgabe stellt sich dann so: Lösungen der Differentialgleichung $\Delta u + k^2 u = 0$ anzugeben, welche auf einer Riemann'schen Fläche eindeutig sind und vorgegebene Unstetigkeiten besitzen. Unsere Fragestellung erinnert an die analoge Aufgabe bei der Differentialgleichung $\Delta u = 0$, deren Lösung bekanntlich die algebraischen Functionen bilden. Diese Analogie führt auch zur

wirklichen Aufstellung der gesuchten Functionen. Man kann nämlich ein Verfahren angeben, durch welches eine Lösung von $\Delta u = 0$ mit gewissen Eigenschaften übergeführt wird in eine Lösung von $\Delta u + k^2 u = 0$ mit entsprechenden Eigenschaften.

Dieses Verfahren wird an zwei einfachen Beispielen erläutert. Ausgehend von den complexen Functionen

$$u = \frac{1}{1-z} \quad \text{bez.} \quad u = \frac{1}{1-\sqrt{z}},$$

gelangt man zu zwei Lösungen unserer Differentialgleichung, von denen die erste aus der Optik wohlbekannt ist und die Ausbreitung von parallelem Licht in der schlichten Ebene darstellt. Die zweite liefert die entsprechende Lichtbewegung auf der zu $\sqrt{z}$ gehörigen Riemann'schen Fläche. Beide Wellenbewegungen werden durch Figuren veranschaulicht.

Man braucht nur zwei Wellen der letzteren Art zu überlagern, um zur Lösung eines wichtigen Beugungsproblemes zu kommen. Zum Zweck der numerischen Rechnung muss man Näherungsformeln aufstellen. Dabei ergeben sich unter gewissen Umständen (bei grossem Beugungswinkel) die Formeln des Herrn Poincaré (Acta Mathematica, Bd. 16), unter anderen Umständen (bei kleinem Beugungswinkel) die nach dem gewöhnlichen Verfahren abgeleiteten Formeln von Kirchhoff.

Eine ausführliche Darstellung dieser Dinge erscheint demnächst in Bd. 47 der Mathematischen Annalen. Vgl. auch zwei Noten in den Nachrichten der Kgl. Gesellschaft der Wissenschaften zu Göttingen: Zur mathematischen Theorie der Beugungserscheinungen, 1894, und: Zur Integration der partiellen Differentialgleichung $\triangle u + k^2 u = 0$ auf Riemann'schen Flächen, 1895.

Die Theorie

der

algebraischen Zahlkörper.

Bericht,

erstattet der Deutschen Mathematiker-Vereinigung

von

David Hilbert.

Vorwort.

Die Zahlentheorie gehört zu den ältesten Zweigen mathematischen Wissens, und es wurde der menschliche Geist sogar auf tief liegende Eigenschaften der natürlichen Zahlen frühzeitig aufmerksam. Doch als selbständige und systematische Wissenschaft ist sie durchaus ein Werk der neueren Zeit.

An der Zahlentheorie werden von jeher die Einfachheit ihrer Grundlagen, die Genauigkeit ihrer Begriffe und die Reinheit ihrer Wahrheiten gerühmt; ihr kommen diese Eigenschaften von Hause aus zu, während andere mathematische Wissenszweige erst eine mehr oder minder lange Entwickelung haben durchmachen müssen, bis die Forderungen der Sicherheit in den Begriffen und der Strenge in den Beweisen überall erfüllt worden sind.

Es nimmt uns daher die hohe Begeisterung nicht Wunder, von der zu allen Zeiten die Jünger dieser Wissenschaft beseelt gewesen sind. „Fast alle Mathematiker, die sich mit der Zahlentheorie beschäftigen“, so sagt *Legendre,* indem er *Euler*'s Liebe zur Zahlentheorie schildert, „geben sich ihr mit einer gewissen Leidenschaft hin“. Weiter erinnern wir uns, welche Verehrung unser Meister *Gauss* für die arithmetische Wissenschaft empfand, wie, als ihm zuerst der Beweis einer ausgezeichneten arithmetischen Wahrheit nach Wunsch gelungen war, „ihn die Reize dieser Untersuchungen so umstrickten, dass er sie nicht mehr lassen konnte“, und wie er *Fermat, Euler, Lagrange* und *Legendre* als „Männer

von unvergleichlichem Ruhme" preist, weil sie „den Zugang zu dem Heiligtume dieser göttlichen Wissenschaft erschlossen und gezeigt haben, von wie grossen Reichtümern es erfüllt ist".

Eine besondere Eigentümlichkeit der Zahlentheorie bildet die oft entgegentretende Schwierigkeit der Beweise einfacher und durch Induction leicht entdeckter Wahrheiten. „Gerade dieses ist es", sagt *Gauss*, „was der höheren Arithmetik jenen zauberischen Reiz giebt, der sie zur Lieblingswissenschaft der ersten Geometer gemacht hat, ihres unerschöpflichen Reichtums nicht zu gedenken, woran sie alle anderen Teile der Mathematik so weit übertrifft."

Bekannt ist auch *Lejeune Dirichlet*'s Vorliebe für die Arithmetik; *Kummer*'s wissenschaftliche Thätigkeit war weitaus in erster Linie der Zahlentheorie geweiht, und *Kronecker* gab dem Empfinden seines mathematischen Herzens Ausdruck durch die Worte: „Die ganze Zahl schuf der liebe Gott, alles Uebrige ist Menschenwerk."

In Anbetracht der Schlichtheit ihrer Voraussetzungen ist sicher die Zahlentheorie der Wissenszweig der Mathematik, dessen Wahrheiten am leichtesten zu begreifen sind. Aber die arithmetischen Begriffe und Beweismethoden erfordern zu ihrer Auffassung und völligen Beherrschung einen hohen Grad von Abstractionsfähigkeit des Verstandes, und dieser Umstand wird bisweilen als ein Vorwurf gegen die Arithmetik geltend gemacht. Ich bin der Meinung, dass alle die anderen Wissensgebiete der Mathematik wenigstens einen gleich hohen Grad von Abstractionsfähigkeit des Verstandes verlangen — vorausgesetzt, dass man auch in diesen Gebieten die Grundlagen überall mit derjenigen Strenge und Vollständigkeit zur Untersuchung zieht, welche thatsächlich notwendig ist.

Was die Stellung der Zahlentheorie innerhalb der gesamten mathematischen Wissenschaft betrifft, so fasst *Gauss* in der Vorrede zu den Disquisitiones arithmeticae die Zahlentheorie noch lediglich als eine Theorie der ganzen natürlichen Zahlen auf mit ausdrücklicher Ausschliessung aller imaginären Zahlen. Dementsprechend rechnet er die Kreisteilung an und für sich nicht zur Zahlentheorie, fügt aber hinzu, dass „ihre Principien einzig und

allein aus der höheren Arithmetik geschöpft werden". Neben *Gauss* geben auch *Jacobi* und *Lejeune Dirichlet* wiederholt und nachdrücklich ihrer Verwunderung Ausdruck über den engen Zusammenhang zahlentheoretischer Fragen mit algebraischen Problemen, insbesondere mit dem Problem der Kreisteilung. Der innere Grund für diesen Zusammenhang ist heute völlig aufgedeckt. Die Theorie der algebraischen Zahlen und die Galois'sche Gleichungstheorie haben nämlich in der allgemeinen Theorie der algebraischen Körper ihre gemeinsame Wurzel, und die Theorie der Zahlkörper insbesondere ist zugleich der wesentlichste Bestandteil der modernen Zahlentheorie geworden.

Das Verdienst, den ersten Keim für die Theorie der Zahlkörper gelegt zu haben, gebührt wiederum *Gauss*. *Gauss* erkannte die natürliche Quelle für die Gesetze der biquadratischen Reste in einer „Erweiterung des Feldes der Arithmetik", wie er sagt, nämlich in der Einführung der ganzen imaginären Zahlen von der Form $a+bi$; er stellte und löste das Problem, alle Sätze der gewöhnlichen Zahlentheorie, vor allem die Teilbarkeitseigenschaften und die Congruenzbeziehungen, auf jene ganzen imaginären Zahlen zu übertragen. Durch die systematische und allgemeine Fortentwickelung dieses Gedankens, auf Grund der neuen weittragenden Ideen *Kummer*'s, gelangten später *Dedekind* und *Kronecker* zu der heutigen Theorie des algebraischen Zahlkörpers.

Aber nicht nur mit der Algebra, sondern auch mit der Functionentheorie steht die Zahlentheorie in innigster wechselseitiger Beziehung. Wir erinnern an die zahlreichen und merkwürdigen Analogien, welche zwischen gewissen Thatsachen aus der Theorie der Zahlkörper und aus der Theorie der algebraischen Functionen einer Veränderlichen bestehen, ferner an die tiefsinnigen Untersuchungen von *Riemann*, durch welche die Beantwortung der Frage nach der Häufigkeit der Primzahlen von der Kenntniss der Nullstellen einer gewissen analytischen Function abhängig gemacht wird. Auch die Transcendenz der Zahlen e und π ist eine arithmetische Eigenschaft einer analytischen Function, nämlich der

Exponentialfunction. Endlich ruht die so wichtige und weittragende, von *Lejeune Dirichlet* ersonnene Methode zur Bestimmung der Klassenanzahl eines Zahlkörpers auf analytischer Grundlage.

Am tiefsten aber berühren die periodischen Functionen und gewisse Functionen mit linearen Transformationen in sich das Wesen der Zahl: so ist die Exponentialfunction $e^{2i\pi z}$ als die Invariante der ganzen rationalen Zahl aufzufassen, insofern sie die Grundlösung der Functionalgleichung $f(z+1)=f(z)$ darstellt. Ferner hatte schon *Jacobi* den engen Zusammenhang zwischen der Theorie der elliptischen Functionen und der Theorie der quadratischen Irrationalitäten empfunden; er giebt sogar der Vermutung Raum, dass bei *Gauss* der oben erwähnte Gedanke der Einführung der ganzen imaginären Zahlen von der Form $a+bi$ nicht auf rein arithmetischem Boden erwachsen ist, sondern durch *Gauss*' gleichzeitige Untersuchungen über die lemniscatischen Functionen und deren complexe Multiplication mitbedingt wurde. Es sind die elliptische Function für geeignete Werte ihrer Perioden und die elliptische Modulfunction jedesmal die Invariante der ganzen Zahl eines bestimmten imaginären quadratischen Zahlkörpers. Diese als Invarianten bezeichneten Functionen vermögen für die bezüglichen Zahlkörper gewisse tiefliegende und schwierige Probleme zur Lösung zu bringen, und umgekehrt verdankt die Theorie der elliptischen Functionen dieser arithmetischen Auffassung und Anwendung einen neuen Aufschwung.

So sehen wir, wie die Arithmetik, die „Königin" der mathematischen Wissenschaft, weite algebraische und functionentheoretische Gebiete erobert und in ihnen die Führerrolle übernimmt. Dass dies aber nicht früher und nicht bereits in noch höherem Maasse geschehen ist, scheint mir daran zu liegen, dass die Zahlentheorie erst in neuester Zeit in ihr reiferes Alter getreten ist. Sogar noch *Gauss* klagt über die unverhältnissmässig grossen Anstrengungen, die ihn die Bestimmung eines Wurzelzeichens in der Zahlentheorie gekostet: es habe ihn „manches Andere wohl nicht so viel Tage aufgehalten, als dieses Jahre", und dann auf ein Mal, „wie der Blitz einschlägt",

habe „sich das Räthsel gelöset“. An Stelle eines solchen für das früheste Alter einer Wissenschaft charakteristischen, sprunghaften Fortschrittes ist heute durch den systematischen Aufbau der Theorie der Zahlkörper eine sichere und stetige Entwickelung getreten.

Es kommt endlich hinzu, dass, wenn ich nicht irre, überhaupt die moderne Entwickelung der reinen Mathematik vornehmlich unter dem Zeichen der Zahl geschieht: *Dedekind*'s und *Weierstrass*' Definitionen der arithmetischen Grundbegriffe und *Cantor*'s allgemeine Zahlgebilde führen zu einer Arithmetisirung der Functionentheorie und dienen zur Durchführung des Princips, dass auch in der Functionentheorie eine Thatsache erst dann als bewiesen gilt, wenn sie in letzter Instanz auf Beziehungen für ganze rationale Zahlen zurückgeführt worden ist. Die Arithmetisirung der Geometrie vollzieht sich durch die modernen Untersuchungen über Nicht-Euklidische Geometrie, in denen es sich um einen streng logischen Aufbau derselben und um die möglichst directe und völlig einwandsfreie Einführung der Zahl in die Geometrie handelt.

Der Zweck des vorliegenden Berichtes ist es, die Thatsachen aus der Theorie der algebraischen Zahlkörper mit ihren Beweisgründen in logischer Entwickelung und nach einheitlichen Gesichtspunkten darzustellen und so mitzuwirken, dass der Zeitpunkt näher komme, wo die Errungenschaften unserer grossen Klassiker der Zahlentheorie Gemeingut aller Mathematiker geworden sind. Historische Erörterungen oder gar Prioritätsuntersuchungen sind ganz vermieden worden. Um die Darstellung auf einem verhältnissmässig so kleinen Raum zu ermöglichen, habe ich mich bemüht, überall den ergiebigsten Quellen nachzuspüren, und ich gab, wenn eine Auswahl sich bot, allemal den schärferen und weiter tragenden Hülfsmitteln den Vorzug. Die Frage, welcher von mehreren Beweisen der einfachste und naturgemässeste ist, lässt sich meist nicht an sich entscheiden, sondern erst die Erwägung, ob die dabei zu Grunde gelegten Principien der Verallge-

meinerung fähig und zur Weiterforschung brauchbar sind, giebt uns eine sichere Antwort.

Der erste Teil des Berichtes behandelt die allgemeine Theorie der algebraischen Zahlkörper; diese Theorie erscheint uns als ein mächtiger Bau, getragen von drei Grundpfeilern: dem Satze von der eindeutigen Zerlegung in Primideale, dem Satze von der Existenz der Einheiten und dem Satze von der transcendenten Bestimmung der Klassenanzahl. Der zweite Teil enthält die Theorie des *Galois*'schen Zahlkörpers, in der auch umgekehrt die Gesetze der allgemeinen Körpertheorie enthalten sind. Der dritte Teil ist dem klassischen Beispiel des quadratischen Körpers gewidmet. Der vierte Teil behandelt den Kreiskörper. Der fünfte Teil endlich entwickelt die Theorie desjenigen Körpers, den *Kummer* bei seinen Untersuchungen über höhere Reciprocitätsgesetze zu Grunde gelegt hat, und den ich desshalb nach diesem Mathematiker benannt habe. Es ist die Theorie dieses *Kummer*'schen Körpers offenbar auf der Höhe des heutigen arithmetischen Wissens die äusserste erreichte Spitze, und man übersieht von ihr aus in weitem Rundblick das ganze durchforschte Gebiet, da fast jeder wesentliche Gedanke und Begriff aus der Körpertheorie, zum wenigsten in specieller Fassung, bei dem Beweise der höheren Reciprocitätsgesetze seine Anwendung findet. Ich habe versucht, den grossen rechnerischen Apparat von *Kummer* zu vermeiden, damit auch hier der Grundsatz von *Riemann* verwirklicht würde, demzufolge man die Beweise nicht durch Rechnung, sondern lediglich durch Gedanken zwingen soll.

Die im dritten, vierten und fünften Teile behandelten Theorien sind sämtlich Theorien besonderer Abel'scher oder relativ-Abel'scher Körper. Ein weiteres Beispiel für eine solche Theorie ist die complexe Multiplication der elliptischen Functionen, indem wir diese als eine Theorie derjenigen Zahlkörper auffassen, welche in Bezug auf einen gegebenen imaginären quadratischen Körper relativ-Abel'sche sind. Die Untersuchungen über die complexe Multiplication der elliptischen Functionen mussten jedoch von der Auf-

nahme in den vorliegenden Bericht ausgeschlossen werden, weil die Thatsachen dieser Theorie noch nicht bis zu dem Grade der Einfachheit und Vollständigkeit ausgearbeitet sind, dass eine befriedigende Darstellung derselben gegenwärtig möglich ist.

Die Theorie der Zahlkörper ist wie ein Bauwerk von wunderbarer Schönheit und Harmonie; als der am reichsten ausgestattete Teil dieses Bauwerkes erscheint mir die Theorie der Abel'schen und relativ-Abel'schen Körper, die uns *Kummer* durch seine Arbeiten über die höheren Reciprocitätsgesetze und *Kronecker* durch seine Untersuchungen über die complexe Multiplication der elliptischen Functionen erschlossen haben. Die tiefen Einblicke, welche die Arbeiten dieser beiden Mathematiker in die genannte Theorie gewähren, zeigen uns zugleich, dass in diesem Wissensgebiete eine Fülle der kostbarsten Schätze noch verborgen liegt, winkend als reicher Lohn dem Forscher, der den Wert solcher Schätze kennt und die Kunst, sie zu gewinnen, mit Liebe betreibt.

Die erwähnten fünf Teile des Berichtes gliedern sich in Capitel und Paragraphen, und in diesen schreitet die Entwickelung in der Weise fort, dass allemal die Sätze und Hülfssätze voranstehen und dann ihre Beweise folgen. Ich denke mir den Leser wie einen Reisenden: die Hülfssätze sind Haltestellen, die Sätze sind grössere Stationen, im Voraus bezeichnet, damit an ihnen das Auffassungsvermögen ausruhen kann. Diejenigen Sätze, die wegen ihrer principiellen Bedeutung an sich Hauptziele sind, oder die als Ausgangspunkte zu weiterem Vordringen in noch unentdecktes Land hervorragend geeignet erscheinen, sind durch cursiven Druck ausgezeichnet; es sind dies die Sätze: 7 (S. 184), 31 (S. 195), 40 (S. 208), 44 (S. 211), 45 (S. 212), 47 (S. 214), 56 (S. 230), 82 (S. 263), 94 (S. 279), 100 (S. 293), 101 (S. 295), 131 (S. 339), 143 (S. 381), 144 (S. 382), 150 (S. 402), 158 (S. 449), 159 (S. 459), 161 (S. 471), 164 (S. 492), 166 (S. 495), 167 (S. 496).

Wegen des genauen Inhaltes und der zur Erhöhung der Uebersicht getroffenen Einrichtungen verweise ich auf die Verzeichnisse

S. IX—S. XVIII und S. 526—S. 546; vor Allem möchte ich hier auf das ganz an den Schluss gestellte Verzeichnis der im Berichte vorkommenden Begriffsnamen aufmerksam machen.

Mein Freund *Hermann Minkowski* hat die Correcturbogen dieses Berichtes einer sorgfältigen Durchsicht unterworfen und auch den grössten Teil des Manuscripts gelesen. Wesentliche und mannichfache Verbesserungen formaler und sachlicher Art erfolgten auf seine Anregung hin, und ich spreche ihm für diese Hülfe meinen herzlichsten Dank aus.

Mein Dank gilt auch meiner Frau, die das ganze Manuscript geschrieben und die Verzeichnisse angefertigt hat.

Endlich gebührt der Redactionscommission der Deutschen Mathematiker-Vereinigung, insbesondere Herrn *A. Gutzmer*, für die Durchsicht der Correcturbogen und der Verlagsbuchhandlung *Georg Reimer* für ihr weitgehendes Entgegenkommen bei Herstellung des Satzes meine dankbare Anerkennung.

Göttingen, den 10. April 1897.

David Hilbert.

Verzeichnis des Inhaltes.

Erster Teil.

Die Theorie des allgemeinen Zahlkörpers.

Capitel I.

Die algebraische Zahl und der Zahlkörper.

Capitel II.

Die Ideale des Zahlkörpers.

Capitel III.

Die Congruenzen nach Idealen.

Capitel IV.

Die Discriminante des Körpers und ihre Teiler.

Capitel V.

Seit

Der Relativkörper.

Capitel VI.

Die Einheiten des Körpers.

Capitel VII.

Die Idealklassen des Körpers.

Capitel VIII.

Die zerlegbaren Formen des Körpers.

Capitel IX.

Die Zahlringe des Körpers.

Seite

Zweiter Teil.

Der Galois'sche Zahlkörper.

Capitel X.

Die Primideale des Galois'schen Körpers und seiner Unterkörper.

Capitel XI.

Die Differenten und Discriminanten des Galois'schen Körpers und seiner Unterkörper.

Capitel XII.

Die Beziehungen der arithmetischen zu algebraischen Eigenschaften des Galois'schen Körpers.

Capitel XIII.

Die Zusammensetzung der Zahlkörper.

Vierter Teil.

Der Kreiskörper.

Capitel XXI.

Die Einheitswurzeln mit Primzahlexponent l und der durch sie bestimmte Kreiskörper.

Seite

Capitel XXII.

Die Einheitswurzeln für einen zusammengesetzten Wurzelexponenten m und der durch sie bestimmte Kreiskörper.

Capitel XXIII.

Der Kreiskörper in seiner Eigenschaft als Abel'scher Körper.

Capitel XXIV.

Die Wurzelzahlen des Kreiskörpers der $l$ten Einheitswurzeln.

Fünfter Teil.

Der Kummer'sche Zahlkörper.

Capitel XXVIII.

Die Zerlegung der Zahlen des Kreiskörpers im Kummer'schen Körper.

Capitel XXIX.

Die Normenreste und Normennichtreste des Kummer'schen Körpers.

Capitel XXX.

Das Vorhandensein unendlich vieler Primideale mit vorgeschriebenen Potenzcharakteren im Kummer'schen Körper.

Capitel XXXI.

Der reguläre Kreiskörper.

Capitel XXXII.

Die ambigen Idealklassen und die Geschlechter im regulären Kummer'schen Körper.

Capitel XXXIII.

Das Reciprocitätsgesetz für $l$te Potenzreste im regulären Kreiskörper.

Erster Teil.

Die Theorie des allgemeinen Zahlkörpers.

Capitel I.

Die algebraische Zahl und der Zahlkörper.

§ 1.

Der Zahlkörper und die conjugirten Zahlkörper.

Eine Zahl α heisst eine **algebraische Zahl,** wenn sie einer Gleichung $m$ten Grades von der Gestalt

$$\alpha^m + a_1 \alpha^{m-1} + a_2 \alpha^{m-2} + \cdots + a_m = 0$$

genügt, wo $a_1, a_2, \ldots, a_m$ rationale Zahlen sind.

Sind $\alpha, \beta, \ldots, \varkappa$ eine endliche Anzahl beliebiger algebraischer Zahlen, so bilden alle rationalen Functionen von $\alpha, \beta, \ldots, \varkappa$ mit ganzzahligen Coefficienten ein in sich abgeschlossenes System von algebraischen Zahlen, welches **Zahlkörper, Körper** oder **Rationalitätsbereich** genannt wird [*Dedekind* [1,2], *Kronecker* [16]]. Da insbesondere die Summe, die Differenz, das Product und der Quotient zweier Zahlen eines Rationalitätsbereiches oder Körpers wieder eine Zahl des Körpers ist, so verhält sich der Begriff des Rationalitätsbereichs oder Körpers gegenüber den 4 Rechnungsoperationen der Addition, Subtraction, Multiplication und Division invariant.

Satz 1. In jedem Körper k giebt es eine Zahl ϑ derart, dass alle anderen Zahlen des Körpers ganze rationale Functionen von ϑ mit rationalen Coefficienten sind.

Der Grad m der Gleichung niedrigsten Grades mit rationalen Coefficienten, der diese Zahl ϑ genügt, heisst der **Grad des Körpers** k. Die Zahl ϑ wird eine **den Körper bestimmende Zahl** genannt. Die Gleichung $m$ten Grades für ϑ ist in dem durch die rationalen Zahlen

bestimmten Rationalitätsbereiche irreducibel. Umgekehrt bestimmt jede Wurzel einer solchen irreducibeln Gleichung einen Zahlkörper $m$ten Grades. Sind $\vartheta', \vartheta'', \ldots, \vartheta^{(m-1)}$ die $m-1$ anderen Wurzeln der Gleichung, so heissen die bezüglich durch $\vartheta', \vartheta'', \ldots, \vartheta^{(m-1)}$ bestimmten Körper k', $k'', \ldots, k^{(m-1)}$ die **zu k conjugirten Körper.** Ist α eine beliebige Zahl des Körpers k, und ist

$$\alpha = c_1 + c_2\vartheta + \cdots + c_m\vartheta^{m-1},$$

wo $c_1, c_2, \ldots, c_m$ rationale Zahlen sind, so heissen die Zahlen

$$\alpha' = c_1 + c_2\vartheta' + \cdots + c_m\vartheta'^{m-1},$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

$$\alpha^{(m-1)} = c_1 + c_2\vartheta^{(m-1)} + \cdots + c_m(\vartheta^{(m-1)})^{m-1}$$

die bez. durch die Substitutionen $t' = (\vartheta : \vartheta'), \ldots, t^{(m-1)} = (\vartheta : \vartheta^{(m-1)})$ aus α entspringenden oder **zu α conjugirten Zahlen.**

§ 2.

Die ganze algebraische Zahl.

Eine algebraische Zahl α heisst eine **ganze algebraische Zahl** oder kurz eine **ganze Zahl,** wenn sie einer Gleichung von der Gestalt

$$\alpha^m + a_1\alpha^{m-1} + a_2\alpha^{m-2} + \cdots + a_m = 0$$

genügt, deren Coefficienten $a_1, a_2, \ldots, a_m$ sämtlich ganze rationale Zahlen sind.

Satz 2. Jede ganze ganzzahlige Function F, d. h. jede ganze rationale Function mit ganzzahligen Coefficienten von beliebig vielen ganzen Zahlen $\alpha, \beta, \ldots, \varkappa$ ist wiederum eine ganze Zahl.

Beweis: Bezeichnen wir mit $\alpha', \alpha'', \ldots, \beta', \beta'', \ldots, \ldots, \varkappa', \varkappa'', \ldots$ bezüglich die zu $\alpha, \beta, \ldots, \varkappa$ conjugirten Zahlen, und bilden wir dann sämtliche Ausdrücke von der Gestalt

$$F(\alpha, \beta, \ldots, \varkappa), \quad F(\alpha', \beta, \ldots, \varkappa), \quad F(\alpha, \beta', \ldots, \varkappa), \quad \ldots,$$
$$\ldots, \quad F(\alpha, \beta, \ldots, \varkappa'), \quad \ldots, \quad F(\alpha', \beta', \ldots, \varkappa), \quad \ldots,$$

so lehrt der bekannte Satz von den symmetrischen Functionen, dass die Gleichung, welcher diese sämtlichen Ausdrücke genügen, lauter ganzzahlige Coefficienten hat, während der Coefficient der höchsten Potenz der Unbekannten $= 1$ ausfällt.

Insbesondere ist die Summe, die Differenz und das Product zweier ganzen Zahlen wiederum eine ganze Zahl. Der Begriff „ganz" verhält sich mithin gegenüber den drei Rechnungsoperationen der Addition, Subtraction und Multiplication invariant. Eine ganze Zahl γ heisst durch

die ganze Zahl α **teilbar,** wenn eine ganze Zahl β existirt, so dass $\gamma = \alpha\beta$ ist.

Satz 3. Die Wurzeln einer Gleichung beliebigen Grades r von der Gestalt

$$\alpha^r + a_1 \alpha^{r-1} + a_2 \alpha^{r-2} + \cdots + a_r = 0$$

sind stets ganze algebraische Zahlen, sobald die Coefficienten $a_1, a_2, \ldots, a_r$ ganze algebraische Zahlen sind.

Satz 4. Wenn eine ganze algebraische Zahl α zugleich rational ist, so ist sie eine ganze rationale Zahl.

Beweis: Wäre nämlich $\alpha = \frac{a}{b}$, wo a und b ganze rationale, zu einander prime Zahlen bedeuten und dabei $b > 1$, und genügt α einer Gleichung, deren Coefficienten $a_1, \ldots, a_m$ ganze rationale Zahlen sind, so würde durch Multiplication dieser Gleichung mit b^{m-1}

$$\frac{a^m}{b} = -a_1 a^{m-1} - a_2 b a^{m-2} - \cdots - a_m b^{m-1} = A$$

folgen, wo A eine ganze rationale Zahl wäre, und dies ist nicht möglich. [*Dedekind*[1], *Kronecker*[16].]

§ 3.

Die Norm, die Differente, die Discriminante einer Zahl. Die Basis des Zahlkörpers.

Ist α eine beliebige Zahl des Körpers k, und bedeuten $\alpha', \ldots, \alpha^{(m-1)}$ die zu α conjugirten Zahlen, so heisst das Product

$$n(\alpha) = \alpha\alpha' \ldots \alpha^{(m-1)}$$

die **Norm der Zahl** α. Die Norm einer Zahl α ist stets eine rationale Zahl. Ferner nenne ich das Product

$$\delta(\alpha) = (\alpha - \alpha')(\alpha - \alpha'') \ldots (\alpha - \alpha^{(m-1)})$$

die **Differente der Zahl** α. Die Differente einer Zahl ist wiederum eine Zahl des Körpers k. Es ist nämlich, wenn zur Abkürzung

$$f(x) = (x - \alpha)(x - \alpha') \ldots (x - \alpha^{(m-1)})$$

gesetzt wird, $\delta(\alpha) = \left[\frac{df(x)}{dx}\right]_{x=\alpha}$. Endlich heisst das Produkt

$$d(\alpha) = (\alpha - \alpha')^2 (\alpha - \alpha'')^2 (\alpha' - \alpha'')^2 \ldots (\alpha^{(m-2)} - \alpha^{(m-1)})^2$$

$$= \begin{vmatrix} 1, & \alpha, & \alpha^2, & \ldots, & \alpha^{m-1} \\ 1, & \alpha', & \alpha'^2, & \ldots, & \alpha'^{m-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1, & \alpha^{(m-1)}, & (\alpha^{(m-1)})^2, & \ldots, & (\alpha^{(m-1)})^{m-1} \end{vmatrix}^2$$

die **Discriminante der Zahl** α. Die Discriminante einer Zahl ist eine rationale Zahl, und zwar bis auf das Vorzeichen gleich der Norm der Differente; es ist nämlich $d(\alpha) = (-1)^{\frac{m(m-1)}{2}} n(\delta)$.

Ist α eine den Körper bestimmende Zahl, so sind ihre Differente und Discriminante verschieden von 0. Umgekehrt, wenn Differente oder Discriminante einer Zahl von 0 verschieden sind, so bestimmt diese den Körper. Ist α eine ganze Zahl, so sind ihre Norm, ihre Differente, ihre Discriminante ebenfalls ganz.

Satz 5. In einem Zahlkörper $m$ten Grades giebt es stets m ganze Zahlen $\omega_1, \omega_2, \ldots, \omega_m$ von der Beschaffenheit, dass jede andere ganze Zahl ω des Körpers sich in der Gestalt

$$\omega = a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m$$

darstellen lässt, wo $a_1, \ldots, a_m$ ganze rationale Zahlen sind.

Beweis. Ist α eine den Körper bestimmende Zahl, so ist jede Zahl ω in der Gestalt

$$\omega = r_1 + r_2\alpha + \cdots + r_m\alpha^{m-1}$$

darstellbar, wo $r_1, r_2, \ldots, r_m$ rationale Zahlen sind. Durch Uebergang zu den conjugirten Zahlen erhält man

$$\omega' = r_1 + r_2\alpha' + \cdots + r_m\alpha'^{m-1},$$

$$\cdots\cdots\cdots\cdots$$

$$\omega^{(m-1)} = r_1 + r_2\alpha^{(m-1)} + \cdots + r_m(\alpha^{(m-1)})^{m-1};$$

und hieraus folgt allgemein für $s = 1, 2, \ldots, m$ in leicht verständlicher Abkürzung:

$$r_s = \frac{|1, \alpha, \ldots, \omega, \ldots, \alpha^{m-1}|}{|1, \alpha, \ldots, \alpha^{s-1}, \ldots, \alpha^{m-1}|}$$

$$= \frac{|1, \alpha, \ldots, \omega, \ldots, \alpha^{m-1}|\,|1, \alpha, \ldots, \alpha^{s-1}, \ldots, \alpha^{m-1}|}{|1, \alpha, \ldots, \alpha^{s-1}, \ldots, \alpha^{m-1}|^2} = \frac{A_s}{d(\alpha)},$$

wo A_s als ganze ganzzahlige Function von $\alpha, \alpha', \ldots, \alpha^{(m-1)}, \omega, \omega', \ldots, \omega^{(m-1)}$ eine ganze Zahl ist. Da andererseits A_s gleich der rationalen Zahl $r_s d(\alpha)$ ist, so ist A_s nach Satz 4 eine ganze rationale Zahl. Jede ganze Zahl ω gestattet daher die Darstellung

$$(1.) \qquad \omega = \frac{A_1 + A_2\alpha + \cdots + A_m\alpha^{m-1}}{d(\alpha)},$$

wo $A_1, A_2, \ldots, A_m$ ganze rationale Zahlen sind und $d(\alpha)$ die Discriminante von α bedeutet.

Nun sei wiederum s eine bestimmte von den Zahlen $1, 2, \ldots, m$; wir denken uns alle ganzen Zahlen des Körpers von der Gestalt

$$\omega_s = \frac{O_1 + O_2\alpha + \cdots + O_s\,\alpha^{s-1}}{d(\alpha)},$$
$$\omega_s^{(1)} = \frac{O_1^{(1)} + O_2^{(1)}\alpha + \cdots + O_s^{(1)}\alpha^{s-1}}{d(\alpha)},$$
$$\omega_s^{(2)} = \frac{O_1^{(2)} + O_2^{(2)}\alpha + \cdots + O_s^{(2)}\alpha^{s-1}}{d(\alpha)},$$
$$\cdots\cdots\cdots\cdots$$

berechnet, wo die Coefficienten O, $O^{(1)}$, $O^{(2)}$, ... sämtlich ganze rationale Zahlen sind; wir können annehmen, dass etwa $O_s \neq 0$ und der grösste gemeinsame Teiler der sämtlichen Zahlen O_s, $O_s^{(1)}$, $O_s^{(2)}$, ... ist. Dann bilden die betreffenden m ersten Zahlen $\omega_1, \ldots, \omega_m$ ein System von der verlangten Beschaffenheit. Ist nämlich eine beliebige ganze Zahl ω in der Gestalt (1.) vorgelegt, so muss nach der eben gemachten Festsetzung $A_m = a_m O_m$ sein, wo a_m eine gewisse ganze rationale Zahl ist; dann aber ist die Differenz $\omega^* = \omega - a_m\omega_m$ von der Gestalt

$$\omega^* = \frac{A_1^* + A_2^*\alpha + \cdots + A_{m-1}^*\alpha^{m-2}}{d(\alpha)}.$$

Hier wird wiederum $A_{m-1}^* = a_{m-1}O_{m-1}$ sein; die Betrachtung der Differenz $\omega^{**} = \omega^* - a_{m-1}\omega_{m-1}$ und die Fortsetzung dieser Schlussweise zeigt die Richtigkeit des Satzes 5.

Die Zahlen $\omega_1, \ldots, \omega_m$ heissen eine Basis des Systems aller ganzen Zahlen des Körpers k, oder kurz eine **Basis des Körpers k**. Jede andere Basis $\omega_1^*, \ldots, \omega_m^*$ des Körpers ist durch Formeln von der Gestalt

$$\omega_1^* = a_{11}\omega_1 + \cdots + a_{1m}\omega_m,$$
$$\cdots\cdots\cdots$$
$$\omega_m^* = a_{m1}\omega_1 + \cdots + a_{mm}\omega_m$$

gegeben, wo die Determinante der ganzzahligen Coefficienten a gleich ± 1 ist. [*Dedekind*[1], *Kronecker*[16].]

Capitel II.

Die Ideale des Zahlkörpers.

§ 4.

Die Multiplication der Ideale und ihre Teilbarkeit. Das Primideal.

Die erste wichtige Aufgabe der Theorie der Zahlkörper ist die Aufstellung der Gesetze über die Zerlegung (Teilbarkeit) der ganzen alge-

braischen Zahlen. Diese Gesetze sind von bewundernswerther Schönheit und Einfachheit. Sie zeigen eine genaue Analogie mit den elementaren Teilbarkeitsgesetzen in der Theorie der ganzen rationalen Zahlen und besitzen die gleiche fundamentale Bedeutung. Sie sind für den besonderen Fall des Kreiskörpers zuerst von *Kummer* entdeckt worden; ihre Ergründung für den allgemeinen Zahlkörper ist das Verdienst von *Dedekind* und *Kronecker*. Die grundlegenden Begriffe dieser Theorie sind folgende:

Ein System von unendlich vielen ganzen algebraischen Zahlen α_1, α_2, ... des Körpers k, welches die Eigenschaft besitzt, dass eine jede lineare Combination $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots$ derselben wiederum dem System angehört, heisst ein **Ideal** $\mathfrak{a}$; dabei bedeuten λ_1, λ_2, ... ganze algebraische Zahlen des Körpers k.

Satz 6. In einem Ideal $\mathfrak{a}$ giebt es stets m Zahlen $\iota_1, \ldots, \iota_m$ von der Art, dass eine jede andere Zahl des Ideals gleich einer linearen Combination derselben von der Gestalt

$$\iota = l_1\iota_1 + \cdots + l_m\iota_m$$

ist, wo $l_1, \ldots, l_m$ ganze rationale Zahlen sind.

Beweis: Es sei s eine bestimmte von den m Zahlen $1, 2, \ldots, m$; dann denken wir uns alle Zahlen des Ideals von der Gestalt

$$\iota_s = J_1\ \omega_1 + \cdots + J_s\omega_s,$$
$$\iota_s^{(1)} = J_1^{(1)}\omega_1 + \cdots + J_s^{(1)}\omega_s,$$
$$\cdots\cdots\cdots$$

aufgestellt, wo J, $J^{(1)}$, ... ganze rationale Zahlen sind, und wir nehmen an, dass etwa $J_s \neq 0$ und der grösste gemeinsame Teiler der sämtlichen Zahlen J_s, $J_s^{(1)}$, ... ist. Dann folgt, wie auf S. 181, dass die m Zahlen $\iota_1, \ldots, \iota_m$ die verlangte Beschaffenheit haben.

Die Zahlen $\iota_1, \ldots, \iota_m$ heissen eine **Basis des Ideals** $\mathfrak{a}$. Jede andere Basis $\iota_1^*, \ldots, \iota_m^*$ des Ideals $\mathfrak{a}$ ist durch Formeln von der Gestalt

$$\iota_1^* = a_{11}\,\iota_1 + \cdots + a_{1m}\,\iota_m,$$
$$\cdots\cdots\cdots$$
$$\iota_m^* = a_{m1}\iota_1 + \cdots + a_{mm}\iota_m$$

gegeben, wo die Determinante der ganzzahligen Coefficienten a gleich ± 1 ist.

Sind $\alpha_1, \ldots, \alpha_r$ irgend r solche Zahlen des Ideals $\mathfrak{a}$, durch deren lineare Combination unter Benutzung ganzer algebraischer Coefficienten λ des Körpers alle Zahlen des Ideals erhalten werden können, so schreibe ich kurz

$$\mathfrak{a} = (\alpha_1, \ldots, \alpha_r).$$

Wenn $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ und $\mathfrak{b} = (\beta_1, \ldots, \beta_s)$ zwei Ideale sind, so werde dasjenige Ideal, welches entsteht, wenn man alle Zahlen $\alpha_1, \ldots, \alpha_r$ und $\beta_1, \ldots, \beta_s$ zusammen nimmt, kurz mit $(\mathfrak{a}, \mathfrak{b})$ bezeichnet, d. h. ich schreibe

$$(\mathfrak{a}, \mathfrak{b}) = (\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s).$$

Ein Ideal, welches alle und nur die Zahlen von der Gestalt $\lambda\alpha$ enthält, wo λ jede beliebige ganze Zahl des Körpers darstellt und α eine bestimmte ganze Zahl des Körpers bedeutet, heisst ein **Hauptideal** und wird mit (α) oder auch kurz mit α bezeichnet, falls eine Verwechselung mit der Zahl α ausgeschlossen erscheint.

Eine jede Zahl α des Ideals $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ heisst **congruent** 0 nach dem Ideal $\mathfrak{a}$ oder in Zeichen:

$$\alpha \equiv 0, \quad (\mathfrak{a}).$$

Wenn die Differenz zweier Zahlen α und β congruent 0 nach $\mathfrak{a}$ ist, so heissen α und β einander congruent nach $\mathfrak{a}$ oder in Zeichen

$$\alpha \equiv \beta, \quad (\mathfrak{a});$$

sonst heissen sie einander **incongruent** oder in Zeichen

$$\alpha \not\equiv \beta, \quad (\mathfrak{a}).$$

Wenn man jede Zahl eines Ideals $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ mit jeder Zahl eines zweiten Ideals $\mathfrak{b} = (\beta_1, \ldots, \beta_s)$ multiplicirt und die so erhaltenen Zahlen linear mittelst beliebiger ganzer algebraischer Coefficienten des Körpers combinirt, so wird das so entstehende neue Ideal das **Product der beiden Ideale** $\mathfrak{a}$ und $\mathfrak{b}$ genannt, d. h. in Zeichen

$$\mathfrak{a}\mathfrak{b} = (\alpha_1\beta_1, \ldots, \alpha_r\beta_1, \ldots, \alpha_1\beta_s, \ldots, \alpha_r\beta_s).$$

Ein Ideal $\mathfrak{c}$ heisst durch das Ideal $\mathfrak{a}$ **teilbar,** wenn ein Ideal $\mathfrak{b}$ existirt derart, dass $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ ist. Ist ein Ideal $\mathfrak{c}$ durch das Ideal $\mathfrak{a}$ teilbar, so sind alle Zahlen von $\mathfrak{c}$ congruent 0 nach dem Ideal $\mathfrak{a}$. Betreffs der Teiler eines Ideals gilt ferner die Thatsache:

Hülfssatz 1. Ein Ideal $\mathfrak{j}$ ist nur durch eine endliche Anzahl von Idealen teilbar.

Beweis. Man bilde die Norm n einer beliebigen Zahl ι $(\neq 0)$ des Ideals $\mathfrak{j}$; ist dann etwa $\mathfrak{a}$ ein Teiler des Ideals $\mathfrak{j}$, so ist offenbar auch die ganze rationale Zahl $n \equiv 0$ nach $\mathfrak{a}$. Die m Basiszahlen von $\mathfrak{a}$ seien von der Gestalt

$$\alpha_1 = a_{11}\,\omega_1 + \cdots + a_{1m}\,\omega_m, \quad \ldots, \quad \alpha_m = a_{m1}\omega_1 + \cdots + a_{mm}\omega_m,$$

wo $a_{11}, \ldots, a_{mm}$ ganze rationale Zahlen sind. Bedeuten $a'_{11}, \ldots, a'_{mm}$ bezüglich die kleinsten positiven Reste der Zahlen $a_{11}, \ldots, a_{mm}$ nach

n, so wird

$$\mathfrak{a} = (a_{11}\omega_1 + \cdots + a_{1m}\omega_m, \ldots, a_{m1}\omega_1 + \cdots + a_{mm}\omega_m)$$
$$= (a'_{11}\omega_1 + \cdots + a'_{1m}\omega_m, \ldots, a'_{m1}\omega_1 + \cdots + a'_{mm}\omega_m, n),$$

und diese letztere Darstellung des Idealteilers $\mathfrak{a}$ lässt unmittelbar die Richtigkeit der Behauptung erkennen.

Ein von 1 verschiedenes Ideal, welches durch kein anderes Ideal teilbar ist, ausser durch das Ideal 1 und durch sich selbst, heisst ein **Primideal**. Zwei Ideale heissen zu einander **prim,** wenn sie ausser 1 keinen gemeinsamen Idealteiler besitzen. Zwei ganze Zahlen α und β, bez. eine ganze Zahl α und ein Ideal $\mathfrak{a}$ heissen zu einander prim, wenn die Hauptideale (α) und (β), bez. das Hauptideal (α) und das Ideal $\mathfrak{a}$ zu einander prim sind. [*Dedekind* [1].]

§ 5.
Die eindeutige Zerlegbarkeit eines Ideals in Primideale.

Es gilt die fundamentale Thatsache:

Satz 7. *Ein jedes Ideal* $\mathfrak{j}$ *lässt sich stets auf eine und nur auf eine Weise als Product von Primidealen darstellen.*

Dedekind hat seinen Beweis dieses Satzes kürzlich von neuem auseinandergesetzt [*Dedekind* [1]]. Das von *Kronecker* eingeschlagene Beweisverfahren beruht auf der von ihm geschaffenen Theorie der einem Zahlkörper zugehörigen algebraischen Formen. Die Bedeutung dieser Formentheorie tritt deutlicher hervor, wenn man zuerst direct die Sätze der Idealtheorie ableitet; hierbei leistet folgender Hülfssatz wesentliche Dienste:

Hülfssatz 2. Wenn die Coefficienten $\alpha_1, \alpha_2, \ldots, \beta_1, \beta_2, \ldots$ der beiden ganzen Functionen einer Veränderlichen x

$$F(x) = \alpha_1 x^r + \alpha_2 x^{r-1} + \cdots,$$
$$G(x) = \beta_1 x^s + \beta_2 x^{s-1} + \cdots$$

ganze algebraische Zahlen sind und die Coefficienten $\gamma_1, \gamma_2, \ldots$ des Productes beider Functionen

$$F(x)\,G(x) = \gamma_1 x^{r+s} + \gamma_2 x^{r+s-1} + \cdots$$

sämtlich durch die ganze Zahl ω teilbar sind, so ist auch jede der Zahlen $\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_2\beta_1, \alpha_2\beta_2, \ldots$ durch ω teilbar. [*Kronecker* [19], *Dedekind* [7], *Mertens* [1], *Hurwitz* [1,2].]

Aus diesem Hülfssatze ergeben sich leicht der Reihe nach die Sätze [*Hurwitz* [1]]:

Satz 8. Zu jedem vorgelegten Ideale $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ lässt sich stets ein Ideal $\mathfrak{b}$ so finden, dass das Product $\mathfrak{a}\mathfrak{b}$ ein Hauptideal wird.

Beweis. Setzt man $F = \alpha_1 u_1 + \cdots + \alpha_r u_r$ und bildet das Product der $m-1$ Formen mit den conjugirten Coefficienten

$$R = (\alpha_1' u_1 + \cdots + \alpha_r' u_r) \cdots (\alpha_1^{(m-1)} u_1 + \cdots + \alpha_r^{(m-1)} u_r)$$
$$= \beta_1 f_1 + \cdots + \beta_s f_s,$$

wo $f_1, \ldots, f_s$ gewisse von einander verschiedene Potenzen und Producte von Potenzen der $u_1, \ldots, u_r$ und wo $\beta_1, \ldots, \beta_s$ ganze Zahlen des Körpers k sind, so ist $FR = nU$, wo n eine ganze rationale Zahl und U eine ganzzahlige Function bedeutet, deren Coefficienten keinen gemeinsamen Teiler haben. Hieraus folgt, dass $n \equiv 0$ nach dem Product der beiden Ideale $\mathfrak{a}$ und $\mathfrak{b} = (\beta_1, \ldots, \beta_s)$ ist. Der Hülfssatz 2 lehrt ferner, dass auch umgekehrt jede Zahl $\alpha_i \beta_h$ sich durch n teilen lässt. Es ist daher $\mathfrak{a}\mathfrak{b} = n$.

Satz 9. Wenn die drei Ideale $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ der Gleichung $\mathfrak{a}\mathfrak{c} = \mathfrak{b}\mathfrak{c}$ genügen, so ist $\mathfrak{a} = \mathfrak{b}$.

Beweis: Es sei $\mathfrak{m}$ ein Ideal von der Art, dass $\mathfrak{c}\mathfrak{m}$ ein Hauptideal (α) wird. Aus der Voraussetzung folgt $\mathfrak{a}\mathfrak{c}\mathfrak{m} = \mathfrak{b}\mathfrak{c}\mathfrak{m}$ oder $\alpha\mathfrak{a} = \alpha\mathfrak{b}$ und mithin $\mathfrak{a} = \mathfrak{b}$.

Satz 10. Wenn alle Zahlen eines Ideals $\mathfrak{c} \equiv 0$ nach dem Ideal $\mathfrak{a}$ sind, so ist $\mathfrak{c}$ durch $\mathfrak{a}$ teilbar.

Beweis: Ist $\mathfrak{a}\mathfrak{m}$ gleich dem Hauptideal (α), so sind alle Zahlen des Ideals $\mathfrak{m}\mathfrak{c}$ durch α teilbar, und mithin giebt es ein Ideal $\mathfrak{b}$ derart, dass $\mathfrak{m}\mathfrak{c} = \alpha\mathfrak{b}$ wird. Folglich ist $\mathfrak{a}\mathfrak{m}\mathfrak{c} = \alpha\mathfrak{a}\mathfrak{b}$, d. h. $\alpha\mathfrak{c} = \alpha\mathfrak{a}\mathfrak{b}$, und folglich $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$.

Satz 11. Wenn das Product zweier Ideale $\mathfrak{a}\mathfrak{b}$ durch das Primideal $\mathfrak{p}$ teilbar ist, so ist wenigstens eines der Ideale $\mathfrak{a}$ und $\mathfrak{b}$ durch $\mathfrak{p}$ teilbar.

Beweis: Wäre $\mathfrak{a}$ nicht durch $\mathfrak{p}$ teilbar, so würde das Ideal $(\mathfrak{a}, \mathfrak{p})$ ein von $\mathfrak{p}$ verschiedenes und zugleich in $\mathfrak{p}$ aufgehendes Ideal, d. h. $= 1$ sein; demnach wäre $1 = \alpha + \pi$, wo α eine Zahl in $\mathfrak{a}$ und π eine Zahl in $\mathfrak{p}$ bedeutet, und hieraus ergiebt sich durch Multiplication mit einer beliebigen Zahl β in $\mathfrak{b}$ die Beziehung $\beta = \alpha\beta + \pi\beta \equiv \alpha\beta$ nach $\mathfrak{p}$. Zufolge der Voraussetzung ist $\alpha\beta \equiv 0$ nach $\mathfrak{p}$ und folglich auch $\beta \equiv 0$ nach $\mathfrak{p}$.

Nunmehr beweist man den Fundamentalsatz 7 der Idealtheorie, wie folgt: Ist $\mathfrak{j}$ nicht selbst ein Primideal, so sei $\mathfrak{j} = \mathfrak{a}\mathfrak{b}$, wo $\mathfrak{a}$ einen von $\mathfrak{j}$ und 1 verschiedenen Teiler von $\mathfrak{j}$ bedeutet. Ist nun einer der Factoren $\mathfrak{a}$ und $\mathfrak{b}$ nicht ein Primideal, so stellen wir denselben in gleicher Weise als Product zweier Ideale dar und erhalten somit $\mathfrak{j} = \mathfrak{a}'\mathfrak{b}'\mathfrak{c}'$, und so fahren wir

fort. Dieses Verfahren bricht notwendig ab; nach Hülfssatz 1 giebt es nämlich nur eine endliche Anzahl von Teilern des Ideals $\mathfrak{j}$. Ist r diese Anzahl, so kann jedenfalls $\mathfrak{j}$ nicht gleich einem Product von mehr als r Factoren sein, da eine Darstellung $\mathfrak{j} = \mathfrak{a}_1 \ldots \mathfrak{a}_{r+1}$ die Existenz der $r+1$ unter einander verschiedenen Idealteiler

$$\mathfrak{a}_1, \quad \mathfrak{a}_1\mathfrak{a}_2, \quad \mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3, \quad \ldots, \quad \mathfrak{a}_1 \ldots \mathfrak{a}_{r+1}$$

bedingen würde. Der letzte Schritt des eingeschlagenen Verfahrens liefert die gewünschte Darstellung

$$\mathfrak{j} = \mathfrak{p}\mathfrak{q} \ldots \mathfrak{l}.$$

Diese Darstellung ist eindeutig. Denn wäre zugleich $\mathfrak{j} = \mathfrak{p}'\mathfrak{q}' \ldots \mathfrak{l}'$, so wird $\mathfrak{j}$ durch $\mathfrak{p}'$ und folglich nach Satz 11 einer der Factoren $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{l}$, etwa $\mathfrak{p}$, durch $\mathfrak{p}'$ teilbar sein, d. h. es wäre $\mathfrak{p} = \mathfrak{p}'$, und folglich ergiebt sich nach Satz 9 die Gleichung $\mathfrak{q} \ldots \mathfrak{l} = \mathfrak{q}' \ldots \mathfrak{l}'$, welche wie die ursprüngliche zu behandeln ist.

Der Fundamentalsatz 7 lässt leicht die folgende Thatsache erkennen:

Satz 12. Ein jedes Ideal $\mathfrak{j}$ des Körpers k kann als grösster gemeinsamer Teiler zweier ganzen Zahlen $\varkappa$, ϱ dargestellt werden.

Beweis. Ist $\varkappa$ eine beliebige durch $\mathfrak{j}$ teilbare ganze Zahl, ϱ jedoch eine solche durch $\mathfrak{j}$ teilbare ganze Zahl, dass $\frac{\varrho}{\mathfrak{j}}$ zu $\frac{\varkappa}{\mathfrak{j}}$ prim ausfällt, so ist $\mathfrak{j} = (\varkappa, \varrho)$.

§ 6.

Die Formen des Zahlkörpers und ihre Inhalte.

Die *Kronecker*'sche Formentheorie [*Kronecker*[16]] erfordert folgende weitere Begriffsbildungen:

Eine ganze rationale Function F von beliebig vielen Veränderlichen $u, v, \ldots$, deren Coefficienten ganze algebraische Zahlen des Körpers k sind, heisst eine **Form des Körpers** k. Werden in einer Form F statt der Coefficienten der Reihe nach bezüglich die conjugirten Zahlen eingesetzt und die so entstehenden sogenannten **conjugirten Formen** $F', \ldots, F^{(m-1)}$ mit einander und mit der ursprünglichen Form F multiplicirt, so ergiebt sich als Product eine ganze Function der Veränderlichen $u, v, \ldots$, deren Coefficienten ganze rationale Zahlen sind; dieselbe werde in der Gestalt

$$n\,U(u, v, \ldots)$$

angenommen, wo n eine positive ganze rationale Zahl und U eine ganze rationale Function bedeutet, deren Coefficienten ganze rationale Zahlen ohne

gemeinsamen Teiler sind. n heisst die **Norm der Form** F. Wenn die Norm n einer Form gleich 1 ist, so heisst die Form eine **Einheitsform.** Eine ganze Function, deren Coefficienten ganze rationale Zahlen ohne gemeinsamen Teiler sind, heisst eine **rationale Einheitsform.** Zwei Formen heissen einander **inhaltsgleich***) (in Zeichen $\backsimeq$), wenn ihr Quotient gleich dem Quotienten zweier Einheitsformen ist. Insbesondere ist jede Einheitsform $\backsimeq 1$. Eine Form H heisst durch die Form F **teilbar,** wenn eine Form G existirt, derart, dass $H \backsimeq FG$ ist. Eine Form P heisst eine **Primform,** wenn P im Sinne der Inhaltsgleichheit durch keine andere Form ausser durch 1 und durch sich selbst teilbar ist.

Die Beziehung der *Kronecker*'schen Formentheorie zur Theorie der Ideale wird klar durch die Bemerkung, dass aus jedem Ideal $\mathfrak{a}=(\alpha_1, \ldots, \alpha_r)$ eine Form F gebildet werden kann, indem man die Zahlen $\alpha_1, \ldots, \alpha_r$ mit beliebigen von einander verschiedenen Producten aus Potenzen der Unbestimmten $u, v, \ldots$ multiplicirt und zu einander addirt. Umgekehrt liefert eine jede Form F mit den Coefficienten $\alpha_1, \ldots, \alpha_r$ ein Ideal $\mathfrak{a}=(\alpha_1, \ldots, \alpha_r)$. Dieses Ideal $\mathfrak{a}$ nenne ich den **Inhalt** der Form F. Dann gilt folgende Thatsache:

Satz 13. Der Inhalt des Productes zweier Formen ist gleich dem Producte ihrer Inhalte.

Beweis. Es seien F und G Formen mit beliebigen Veränderlichen und den Coefficienten $\alpha_1, \ldots, \alpha_r$ bezüglich $\beta_1, \ldots, \beta_s$, und es sei das Product $H = FG$ eine Form mit den Coefficienten $\gamma_1, \ldots, \gamma_t$. Ferner sei $\mathfrak{p}^a$ die höchste in $\mathfrak{a}=(\alpha_1, \ldots, \alpha_r)$ und $\mathfrak{p}^b$ die höchste in $\mathfrak{b}=(\beta_1, \ldots, \beta_s)$ aufgehende Potenz des Primideals $\mathfrak{p}$. Man denke sich ferner die Glieder der beiden Formen F und G zunächst nach absteigenden Potenzen von u und dann die mit der nämlichen Potenz von u multiplicirten Glieder nach absteigenden Potenzen von v geordnet u. s. f. Bei dieser Anordnung sei $\alpha u^h v^l \ldots$ das erste in F vorkommende Glied, dessen Coefficient α durch keine höhere als die $a$te Potenz von $\mathfrak{p}$, und andererseits sei $\beta u^{h'} v^{l'} \ldots$ das erste in G vorkommende Glied, dessen Coefficient β durch keine höhere als die $b$te Potenz von $\mathfrak{p}$ teilbar ist: dann ist offenbar der Coefficient γ des Gliedes $\gamma u^{h+h'} v^{l+l'} \ldots$ in H durch keine höhere als die $(a+b)$te Potenz von $\mathfrak{p}$ teilbar. Alle übrigen Coefficienten von H sind aber gewiss auch durch $\mathfrak{p}^{a+b}$ teilbar. Somit folgt die Behauptung $(\alpha_1, \ldots, \alpha_r)(\beta_1, \ldots, \beta_s) = (\gamma_1, \ldots, \gamma_t)$.

Aus Satz 13 folgt insbesondere leicht, dass eine jede Einheitsform

*) Nach *Kronecker* „äquivalent in engerem Sinne“.

den Inhalt 1 besitzt, und dass umgekehrt jede Form, deren Coefficienten den grössten gemeinsamen Idealteiler 1 haben, eine Einheitsform ist. Mithin haben inhaltsgleiche Formen stets den nämlichen Inhalt, und umgekehrt sind alle Formen von dem nämlichen Inhalt einander inhaltsgleich. Speciell sind zwei beliebige Formen mit gleichen Coefficienten stets einander inhaltsgleich.

Weitere Folgerungen aus Satz 13 sind:

Satz 14. Wenn F eine vorgelegte Form ist, so lässt sich dazu stets eine Form finden derart, dass FR einer ganzen Zahl inhaltsgleich ist.

Satz 15. Wenn das Product zweier Formen durch eine Primform P teilbar ist, so ist wenigstens eine der beiden Formen durch P teilbar.

Satz 16. Jede Form ist im Sinne der Inhaltsgleichheit auf eine und nur auf eine Weise als Product von Primformen darstellbar.

Diese Sätze laufen parallel bezüglich mit den Sätzen 8, 11 und dem Fundamentalsatze 7 der Idealtheorie.

Ausser den von *Dedekind* und *Kronecker* eingeschlagenen Wegen führen noch zwei einfachere Methoden zum Beweise des Fundamentalsatzes 7; der einen Methode liegt die Theorie des Galois'schen Zahlkörpers zu Grunde. Vgl. § 36 [*Hilbert*[1, 2]]. Die zweite Methode geht von dem Satze aus, dass sich die Ideale eines Körpers auf eine endliche Anzahl von Idealklassen verteilen. Der zum Beweise dieses Satzes erforderliche Grundgedanke kann als eine Verallgemeinerung desjenigen Ansatzes angesehen werden, auf welchem das bekannte Euklidische Divisionsverfahren zur Bestimmung des grössten gemeinsamen Teilers zweier ganzen rationalen Zahlen beruht. [*Hurwitz*[3].]

Capitel III.

Die Congruenzen nach Idealen.

§ 7.

Die Norm eines Ideals und ihre Eigenschaften.

Die in Capitel II entwickelte Theorie der Zerlegung der Ideale eines Körpers gestattet es, die elementaren Sätze der Theorie der rationalen Zahlen auf die Zahlen eines algebraischen Zahlkörpers zu übertragen. Wir stellen folgende allgemeine Begriffe und Sätze voran.

Die Anzahl aller nach einem Ideal $\mathfrak{a}$ einander incongruenten ganzen Zahlen des Körpers heisst die **Norm des Ideals** $\mathfrak{a}$: in Zeichen $n(\mathfrak{a})$.

Satz 17. Die Norm eines Primideals $\mathfrak{p}$ ist eine Potenz der durch $\mathfrak{p}$ teilbaren rationalen Primzahl p.

Beweis. Es seien die f ganzen Zahlen $\omega_1, \ldots, \omega_f$ einer Basis des Körpers in dem Sinne von einander unabhängig, dass keine Congruenz von der Gestalt

$$a_1\omega_1 + \cdots + a_f\omega_f \equiv 0, \quad (\mathfrak{p})$$

besteht, wo $a_1, \ldots, a_f$ ganze, nicht sämtlich durch p teilbare Zahlen bedeuten, und es möge überdies jede der anderen $m-f$ Zahlen der Körperbasis einem Ausdruck von der Gestalt $a_1\omega_1 + \cdots + a_f\omega_f$ nach $\mathfrak{p}$ congruent sein; dann kann dieser Ausdruck jeder Zahl nach $\mathfrak{p}$ congruent werden, und es beträgt die Anzahl der einander incongruenten Zahlen nach $\mathfrak{p}$ offenbar p^f.

Der Exponent f heisst der **Grad des Primideals** $\mathfrak{p}$.

Satz 18. Die Norm des Productes zweier Ideale $\mathfrak{a}\mathfrak{b}$ ist gleich dem Product ihrer Normen.

Beweis. Es sei α eine durch $\mathfrak{a}$ teilbare Zahl von der Art, dass $\frac{\alpha}{\mathfrak{a}}$ ein zu $\mathfrak{b}$ primes Ideal ist. Durchläuft dann ξ ein System von $n(\mathfrak{a})$ nach $\mathfrak{a}$ einander incongruenten Zahlen und η ein System von $n(\mathfrak{b})$ nach $\mathfrak{b}$ zu einander incongruenten Zahlen, so stellt der Ausdruck $\alpha\eta + \xi$ ein volles System nach $\mathfrak{a}\mathfrak{b}$ einander incongruenten Zahlen dar; ein solches System umfasst mithin $n(\mathfrak{a})n(\mathfrak{b})$ Zahlen.

Satz 19. Ist

$$\iota_1 = a_{11}\omega_1 + \cdots + a_{1m}\omega_m,$$
$$\cdots\cdots\cdots\cdots$$
$$\iota_m = a_{m1}\omega_1 + \cdots + a_{mm}\omega_m$$

eine Basis des Ideals $\mathfrak{a}$, so ist seine Norm $n(\mathfrak{a})$ gleich dem absoluten Betrage der Determinante der Coefficienten a.

Beweis. Legen wir die Basis des Ideals in der ursprünglich beim Beweise des Satzes 6 gefundenen Gestalt zu Grunde, wo die Coefficienten a_{rs} für $s > r$ sämtlich $= 0$ sind, so ist die Determinante jener Coefficienten a gleich dem Product $a_{11} \ldots a_{mm}$. Andererseits stellt der Ausdruck

$$u_1\omega_1 + \cdots + u_m\omega_m$$

für

$$u_1 = 0,\ 1,\ \ldots,\ a_{11} - 1,\quad \ldots,\quad u_m = 0,\ 1,\ \ldots,\ a_{mm} - 1$$

ein System nach $\mathfrak{a}$ einander incongruenter Zahlen dar. Damit ist Satz 19 bewiesen. Zugleich leuchtet die Umkehrung dieses Satzes ein.

Der Zusammenhang mit der *Kronecker*'schen Formentheorie erhellt aus dem Satze:

Satz 20. Ist F eine Form mit dem Inhalte $\mathfrak{a}$, so ist die Norm der Form F gleich der Norm des Ideals $\mathfrak{a}$, d. h. $n(F) = n(\mathfrak{a})$. Insbesondere ist die Norm einer ganzen Zahl α dem absoluten Betrage nach stets gleich der Norm des Hauptideals $\mathfrak{a} = (\alpha)$.

Beweis: Ist $\iota_1, \ldots, \iota_m$ eine Basis des Ideals $\mathfrak{a}$, so bilde man die Form

$$F = \iota_1 u_1 + \cdots + \iota_m u_m;$$

dann ist

$$\begin{aligned} \omega_1 F &= l_{11}\iota_1 + \cdots + l_{1m}\iota_m, \\ &\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \omega_m F &= l_{m1}\iota_1 + \cdots + l_{mm}\iota_m, \end{aligned}$$

wo $l_{11}, \ldots, l_{mm}$ lineare Formen von $u_1, \ldots, u_m$ mit ganzen rationalen Coefficienten sind. Wir beweisen zunächst, dass die Determinante $|l_{rs}|$ der Formen $l_{11}, \ldots, l_{mm}$ eine rationale Einheitsform ist. In der That, wären im Gegenteil die Coefficienten der Determinante $|l_{rs}|$ sämtlich durch eine Primzahl p teilbar, so müssten notwendig m Formen $L_1, \ldots, L_m$ existiren, deren Coefficienten ganze rationale, nicht sämtlich durch p teilbare Zahlen sind, und welche den Bedingungen

$$\begin{aligned} L_1 l_{11} + \cdots + L_m l_{m1} &\equiv 0, \quad (p) \\ &\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ L_1 l_{1m} + \cdots + L_m l_{mm} &\equiv 0, \quad (p) \end{aligned}$$

genügen. Hieraus würde

$$(L_1\omega_1 + \cdots + L_m\omega_m)F \equiv 0, \quad (p\mathfrak{a})$$

folgen, d. h. das Product $\mathfrak{l}\mathfrak{a}$ ist durch $p\mathfrak{a}$ teilbar, wobei $\mathfrak{l}$ den Inhalt der Form $L_1\omega_1 + \cdots + L_m\omega_m$ bezeichnet. Mithin wäre $\mathfrak{l}$ durch p teilbar, was nicht der Fall sein kann, da eine Zahl von der Gestalt $a_1\omega_1 + \cdots + a_m\omega_m$, wo $a_1, \ldots, a_m$ ganze rationale Zahlen bedeuten, nur dann durch p teilbar ist, sobald die Coefficienten $a_1, \ldots, a_m$ sämtlich durch p teilbar sind.

Nach dem Multiplicationstheorem der Determinanten ist

$$\begin{vmatrix} \omega_1 F, & \ldots, \omega_m F \\ \omega_1' F', & \ldots, \omega_m' F' \\ \cdot \quad \cdot \quad \cdot & \cdot \quad \cdot \quad \cdot \\ \omega_1^{(m-1)} F^{(m-1)}, & \ldots, \omega_m^{(m-1)} F^{(m-1)} \end{vmatrix} = \begin{vmatrix} l_{11}, \ldots, l_{1m} \\ l_{21}, \ldots, l_{2m} \\ \cdot \quad \cdot \quad \cdot \\ l_{m1}, \ldots, l_{mm} \end{vmatrix} \cdot \begin{vmatrix} \iota_1, & \ldots, \iota_m \\ \iota_1', & \ldots, \iota_m' \\ \cdot \quad \cdot \quad \cdot & \cdot \quad \cdot \\ \iota_1^{(m-1)}, & \ldots, \iota_m^{(m-1)} \end{vmatrix},$$

und mithin folgt nach Weghebung des Factors

$$\begin{vmatrix} \omega_1, & \ldots, & \omega_m \\ \omega_1', & \ldots, & \omega_m' \\ \cdot \quad \cdot & \cdot \quad \cdot & \cdot \\ \omega_1^{(m-1)}, & \ldots, & \omega_m^{(m-1)} \end{vmatrix}$$

die Beziehung $FF' \ldots F^{(m-1)} \sim n(\mathfrak{a})$ oder $n(F) = n(\mathfrak{a})$. Der zweite Teil des Satzes folgt, wenn wir $F = \alpha$ nehmen.

Wendet man auf die sämtlichen Zahlen $\alpha_1, \alpha_2, \ldots$ des Ideals $\mathfrak{a}$ die Substitution $t' = (\vartheta : \vartheta')$ an, so heisst das dann entstehende Ideal $\mathfrak{a}' = (t'\alpha_1, t'\alpha_2, \ldots)$ das durch t' aus $\mathfrak{a}$ entspringende oder **zu $\mathfrak{a}$ conjugirte Ideal.** Betrachtet man den aus $k, k', \ldots, k^{(m-1)}$ zusammengesetzten Körper, so lehren die Sätze 18 und 20, dass das Product von $\mathfrak{a}$ und allen zu $\mathfrak{a}$ conjugirten Idealen eine ganze rationale Zahl, nämlich $n(\mathfrak{a})$ ist. Aus diesem Umstande entspringt eine neue Definition der Norm des Ideals $\mathfrak{a}$, welche der Definition der Norm einer Zahl α genau entspricht und überdies einer wichtigen Verallgemeinerung fähig ist. Vgl. § 14.

Satz 21. In einem jeden Ideal $\mathfrak{j}$ lassen sich stets zwei Zahlen finden, deren Normen die Norm des Ideals $\mathfrak{j}$ zum grössten gemeinsamen Teiler haben.

Beweis. Man setze $a = n(\mathfrak{j})$ und bestimme eine Zahl α in $\mathfrak{j}$ derart, dass $\frac{\alpha}{\mathfrak{j}}$ prim zu a ausfällt. Dann wird, wenn $\alpha', \ldots, \alpha^{(m-1)}$ die zu α conjugirten Zahlen und $\mathfrak{j}', \ldots, \mathfrak{j}^{(m-1)}$ die zu $\mathfrak{j}$ conjugirten Ideale bedeuten, auch $\frac{\alpha'}{\mathfrak{j}'}, \ldots, \frac{\alpha^{(m-1)}}{\mathfrak{j}^{(m-1)}}$, und folglich $\frac{n(\alpha)}{n(\mathfrak{j})} = \frac{n(\alpha)}{a}$ prim zu a, d. h. es ist $n(\mathfrak{j}) = a = (a^m, n(\alpha)) = (n(a), n(\alpha))$.

§ 8.

Der Fermat'sche Satz in der Idealtheorie und die Function $\varphi(\mathfrak{a})$.

Auf Grund der nämlichen Schlüsse wie in der Theorie der rationalen Zahlen ergiebt sich die folgende, dem Fermat'schen Lehrsatz entsprechende Thatsache: [*Dedekind* [1].]

Satz 22. Ist $\mathfrak{p}$ ein Primideal vom Grade f, so genügt jede ganze Zahl ω des Körpers k der Congruenz

$$\omega^{p^f} \equiv \omega, \quad (\mathfrak{p})$$

Auch der verallgemeinerte Fermat'sche Lehrsatz ist leicht auf die Körpertheorie übertragbar. Man beweist ferner ohne Mühe die folgenden Sätze: [*Dedekind*[1].]

Satz 23. Die Anzahl aller derjenigen nach einem Ideale $\mathfrak{a}$ einander incongruenten Zahlen, welche prim zu $\mathfrak{a}$ sind, ist

$$\varphi(\mathfrak{a}) = n(\mathfrak{a})\left(1-\frac{1}{n(\mathfrak{p}_1)}\right)\left(1-\frac{1}{n(\mathfrak{p}_2)}\right)\cdots\left(1-\frac{1}{n(\mathfrak{p}_r)}\right),$$

wo $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ die sämtlichen in $\mathfrak{a}$ aufgehenden und von einander verschiedenen Primideale bedeuten. Für die Zahl φ gelten die beiden Formeln

$$\varphi(\mathfrak{a})\varphi(\mathfrak{b}) = \varphi(\mathfrak{a}\mathfrak{b}) \quad \text{und} \quad \Sigma\varphi(\mathfrak{t}) = n(\mathfrak{a});$$

in der letzteren erstreckt sich die Summation auf alle Idealteiler $\mathfrak{t}$ des Ideals $\mathfrak{a}$.

Satz 24. Jede zu dem Ideal $\mathfrak{a}$ prime ganze Zahl ω genügt der Congruenz

$$\omega^{\varphi(\mathfrak{a})} \equiv 1, \quad (\mathfrak{a}).$$

So genügt beispielsweise jede durch ein Primideal $\mathfrak{p}$ vom Grade f nicht teilbare ganze Zahl ω des Körpers k der Congruenz

$$\omega^{p^f(p^f-1)} \equiv 1, \quad (\mathfrak{p}^2).$$

Es gelten ferner die Thatsachen:

Satz 25. Wenn $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ Ideale bedeuten, von denen stets je zwei zu einander prim sind, und wenn $\alpha_1, \ldots, \alpha_r$ beliebige ganze Zahlen sind, so giebt es eine ganze Zahl ω, die den Congruenzen

$$\omega \equiv \alpha_1, \quad (\mathfrak{a}_1); \quad \ldots, \qquad \omega \equiv \alpha_r, \quad (\mathfrak{a}_r)$$

genügt.

Satz 26. Eine Congruenz $r$ten Grades nach dem Primideal $\mathfrak{p}$ von der Gestalt

$$\alpha x^r + \alpha_1 x^{r-1} + \cdots + \alpha_r \equiv 0, \quad (\mathfrak{p})$$

wo $\alpha, \alpha_1, \ldots, \alpha_r$ ganze Zahlen in k sind, besitzt höchstens r nach $\mathfrak{p}$ einander incongruente Wurzeln.

Satz 27. Bedeutet $\mathfrak{p}$ ein in der rationalen Primzahl p aufgehendes Primideal, und ist α eine Wurzel der Congruenz

$$a x^r + a_1 x^{r-1} + \cdots + a_r \equiv 0, \quad (\mathfrak{p})$$

wo $a, a_1, \ldots, a_r$ ganze rationale Zahlen bedeuten, so ist auch α^p eine Wurzel dieser Congruenz.

Beweis. Bezeichnen wir die linke Seite der obigen Congruenz mit $F(x)$, so gilt nach dem Fermat'schen Satze identisch in x die Congruenz $F(x^p) \equiv (F(x))^p$ nach p, und diese Thatsache bedingt die Richtigkeit der Behauptung.

Das Perpetuum Mobile. By F. ICHAK. Bändchen 462 of the series: Aus Natur und Geisteswelt. Leipzig, Teubner, 1914. 104 pp. Price M. 1.25

THE question of perpetual motion has interested mankind for many centuries. The author says: "We see before us an almost endless series of attempts of different sorts which have one thing in common—a negative result. But mankind does not let itself be convinced of the impossibility of the undertaking by these unnumbered failures: here the wish is mightier than the judgment."

This little book does not claim to be an exhaustive treatise on the subject, but does cover the field remarkably well in such short space. This is largely due to the systematic arrangement of the material. Perpetual motion is discussed under three heads: first, that perpetual motion which depends upon the creation of energy by some device, and this is what is usually meant by perpetual motion; second, that which does not create energy but transforms it from one form to another in some cycle; and third, that motion which is not perpetual but of indefinite length, like the motion of the radium clock. The first of these is the oldest and has been the goal of the greatest number of perpetual motion seekers. The efforts to make a device for the creation of energy which could be utilized in doing work are discussed under several types, such as mechanical, magnetic, hydraulic perpetual motion, etc. Type machines and machines which have attracted unusual attention are described in detail and often illustrated. The effect of learning and the development of science upon the efforts at finding such a machine are discussed as well as the reaction of these experiments on science. With the theory of the conservation of energy came the attempts to secure perpetual motion of the second sort mentioned. The perpetual motion machines of the third sort, or apparent perpetual motion machines, like the radium clock or the radiometer, do not create energy but have it furnished from nature, and while the supply is very great it is not inexhaustible. The author closes with a section on perpetual motion in the future, in which among other things is mentioned the possibility of getting around the difficulties of the conservation of energy by a new theory concerning energy. There is also a prophecy, likely to be fulfilled, that we shall always have the perpetual motion seekers with us.

THOS. E. MASON.

bedeuten, so stellt, wie leicht ersichtlich, die Summe

$$\alpha_1 + \alpha_2 P(\varrho) + \cdots + \alpha_l \{P(\varrho)\}^{l-1}$$

lauter nach $\mathfrak{p}^l$ einander incongruente ganze Zahlen dar, und da hier p^{fl} Zahlen vorliegen, so sind damit sämtliche nach $\mathfrak{p}^l$ incongruenten Reste erschöpft. Offenbar kommt die gleiche Eigenschaft auch jeder Zahl zu, welche der Zahl ϱ nach $\mathfrak{p}^2$ congruent ist.

Den letzteren Umstand benutzen wir zu der folgenden Darstellung des Ideals $\mathfrak{p}$:

Satz 30. Wenn ein Primideal $\mathfrak{p}$ vom $f$ten Grade vorgelegt ist, so giebt es im Körper k stets eine ganze Zahl ϱ von der im Satze 29 verlangten Eigenschaft und überdies von der Art, dass man

$$\mathfrak{p} = (p,\ P(\varrho))$$

hat, wo $P(\varrho)$ eine ganze Function $f$ten Grades von ϱ mit ganzen rationalen Coefficienten ist.

Beweis: Es sei $p = \mathfrak{p}^e \mathfrak{a}$, wo das Ideal $\mathfrak{a}$ nicht durch $\mathfrak{p}$ teilbar ist. Ferner sei α eine nicht durch $\mathfrak{p}$, wohl aber durch $\mathfrak{a}$ teilbare ganze Zahl. Nach Satz 24 ist $\alpha^{p^f(p^f-1)} \equiv 1$ nach $\mathfrak{p}^2$. Ersetzen wir nun die im vorigen Beweise gefundene Zahl ϱ durch $\varrho\alpha^{p^f(p^f-1)}$, so behält diese neue Zahl ϱ die frühere Eigenschaft; da ferner der letzte Coefficient der Function $P(\varrho)$ nicht durch p teilbar sein kann, so ist für die neue Zahl ϱ notwendig $P(\varrho)$ prim zu $\mathfrak{a}$, d. h. $\mathfrak{p} = (p, P(\varrho))$.

Capitel IV.

Die Discriminante des Körpers und ihre Teiler.

§ 10.

Der Satz über die Teiler der Discriminante des Körpers. Hülfssätze über ganze Functionen.

Die **Discriminante** des Körpers k ist, wenn $\omega_1, \ldots, \omega_m$ eine Basis von k bedeutet, definirt durch die Gleichung

$$d = \begin{vmatrix} \omega_1, & \ldots, & \omega_m \\ \omega_1', & \ldots, & \omega_m' \\ \cdot & \cdot & \cdot \\ \omega_1^{(m-1)}, & \ldots, & \omega_m^{(m-1)} \end{vmatrix}^2;$$

sie ist eine ganze rationale Zahl. Für die Entwickelung der Körpertheorie ist die Untersuchung der in der Discriminante des Körpers k aufgehenden idealen Factoren von grundlegender Bedeutung. Es gilt der fundamentale Satz:

Satz 31. *Die Discriminante d des Zahlkörpers k enthält alle und nur diejenigen rationalen Primzahlen als Factoren, welche durch das Quadrat eines Primideals teilbar sind.*

Der Beweis dieses Satzes hat erhebliche Schwierigkeiten verursacht; er ist zum ersten Mal von *Dedekind* geführt worden [*Dedekind*[6]]. *Hensel* hat einen zweiten Beweis dieses Satzes gegeben und dadurch die *Kronecker*sche Theorie der algebraischen Zahlen in einem wesentlichen Punkte ergänzt. Der *Hensel*'sche Beweis beruht auf folgenden von *Kronecker* geschaffenen Begriffen: [*Kronecker*[16], *Hensel*[4].]

Bedeuten $u_1, \ldots, u_m$ Unbestimmte, und ist $\omega_1, \ldots, \omega_m$ eine Basis, so heisst

$$\xi = \omega_1 u_1 + \cdots + \omega_m u_m$$

die **Fundamentalform** des Körpers k. Dieselbe genügt offenbar der Gleichung für x

$$(x - \omega_1 u_1 - \cdots - \omega_m u_m)(x - \omega_1' u_1 - \cdots - \omega_m' u_m) \cdots$$
$$\cdots (x - \omega_1^{(m-1)} u_1 - \cdots - \omega_m^{(m-1)} u_m) = 0,$$

welche die Gestalt

$$x^m + U_1 x^{m-1} + U_2 x^{m-2} + \cdots + U_m = 0$$

annimmt, wo $U_1, \ldots, U_m$ gewisse ganze Functionen von $u_1, \ldots, u_m$ mit ganzen rationalen Coefficienten sind. Diese Gleichung $m$ten Grades heisst die **Fundamentalgleichung.** Um mit den eben definirten Begriffen operiren zu können, ist es nötig, die Sätze über die Zerlegung von ganzen Functionen einer Veränderlichen x nach einer rationalen Primzahl p [*Serret*[1]] auf den allgemeineren Fall zu übertragen, wo die ganzen Functionen neben der einen Veränderlichen x noch die m Unbestimmten $u_1, \ldots, u_m$ als Parameter enthalten.

Im Folgenden werde unter einer **ganzzahligen Function** stets eine solche ganze rationale Function der Veränderlichen oder Unbestimmten verstanden, deren Coefficienten ganze rationale Zahlen sind. Es heisse ferner eine ganzzahlige Function $Z(x; u_1, \ldots, u_m)$ durch eine andere ganzzahlige Function X **teilbar nach** p, wenn eine dritte ganzzahlige Function Y existirt derart, dass identisch in den Veränderlichen $x, u_1, \ldots, u_m$ die Congruenz

$$Z \equiv XY, \quad (p)$$

besteht. Ist eine ganzzahlige Function P nach p durch keine andere Function teilbar ausser durch solche Functionen, die einer ganzen rationalen

Zahl oder der Function P selbst nach p congruent sind, so heisst die Function P eine **Primfunction nach** p. Wie in der Theorie der Functionen einer Veränderlichen gelten auch hier die gewöhnlichen Gesetze der Teilbarkeit; insbesondere heben wir den durch das bekannte *Euklidische* Recursionsverfahren leicht zu beweisenden Satz hervor:

Satz 32. Wenn zwei ganzzahlige Functionen X und Y von x, $u_1, \ldots, u_m$ nach der rationalen Primzahl p keinen gemeinsamen Teiler in x haben, so giebt es eine ganzzahlige, nach p nicht der 0 congruente Function U von $u_1, \ldots, u_m$ allein, so dass man

$$U \equiv AX + BY, \quad (p)$$

hat, wo A und B geeignete ganzzahlige Functionen von $x, u_1, \ldots, u_m$ sind.

Unser nächstes Ziel ist die Zerlegung der linken Seite F der Fundamentalgleichung in Primfunctionen nach der rationalen Primzahl p. Wir beweisen zunächst folgende Hülfssätze:

Hülfssatz 3. Wenn $\mathfrak{p}$ ein in p aufgehendes Primideal $f$ten Grades bezeichnet, so giebt es stets nach p eine Primfunction $\Pi(x; u_1, \ldots, u_m)$ vom $f$ten Grade in x, welche, wenn man an Stelle von x die Fundamentalform ξ setzt, folgende Eigenschaften besitzt: die Coefficienten der Potenzen und Producte von $u_1, \ldots, u_m$ in der Function $\Pi(\xi; u_1, \ldots, u_m)$ sind durch $\mathfrak{p}$, aber nicht sämtlich durch $\mathfrak{p}^2$ und auch nicht sämtlich durch ein von $\mathfrak{p}$ verschiedenes, in p aufgehendes Primideal teilbar.

Beweis. Es sei $p = \mathfrak{p}^e \mathfrak{a}$, wo das Ideal $\mathfrak{a}$ nicht mehr durch $\mathfrak{p}$ teilbar ist. Ferner sei ϱ eine solche Primitivzahl nach $\mathfrak{p}$, welche die in den Sätzen 29 und 30 angegebenen Eigenschaften besitzt. $P(\varrho)$ sei eine wie dort bestimmte, zu $\mathfrak{p}$ gehörige ganzzahlige Function $f$ten Grades von der Art, dass $\mathfrak{p} = (p, P(\varrho))$ ist. $P(x)$ ist Primfunction nach p, weil sonst ϱ einer Congruenz niederen als $f$ten Grades nach $\mathfrak{p}$ genügen würde. Wir setzen

$$\varrho = a_1 \omega_1 + \cdots + a_m \omega_m,$$

wo $a_1, \ldots, a_m$ ganze rationale Zahlen sind, und nehmen den Coefficienten von ϱ^f in $P(\varrho)$ gleich 1 an. Da $P(\varrho) \equiv 0$ nach $\mathfrak{p}$ ist, so folgt nach Satz 27, dass auch $P(\varrho^p) \equiv 0$, $P(\varrho^{p^2}) \equiv 0, \ldots, P(\varrho^{p^{f-1}}) \equiv 0$ nach $\mathfrak{p}$ ist, d. h. die Congruenz $P(x) \equiv 0$ nach $\mathfrak{p}$ besitzt die f einander incongruenten Wurzeln $\varrho, \varrho^p, \ldots, \varrho^{p^{f-1}}$, und es ist mithin identisch in x

$$P(x) \equiv (x - \varrho)(x - \varrho^p) \ldots (x - \varrho^{p^{f-1}}), \quad (\mathfrak{p})$$

d. h. die elementarsymmetrischen Functionen von $\varrho, \varrho^p, \ldots, \varrho^{p^{f-1}}$ sind sämtlich nach $\mathfrak{p}$ gewissen ganzen rationalen Zahlen congruent.

Da jede ganze Zahl des Körpers k nach $\mathfrak{p}$ einer ganzzahligen Function von ϱ congruent ist, so können wir die Fundamentalform

$$\xi \equiv L(\varrho;\, u_1, \ldots, u_m)$$

nach $\mathfrak{p}$ setzen, wo L eine ganzzahlige Function von $\varrho, u_1, \ldots, u_m$ bedeutet. Nach dem eben Bewiesenen ist der Ausdruck

$$(x-L(\varrho;\, u_1, \ldots, u_m))(x-L(\varrho^p;\, u_1, \ldots, u_m))\ldots$$
$$\ldots(x-L(\varrho^{p^{f-1}};\, u_1, \ldots, u_m))$$

nach $\mathfrak{p}$ einer ganzzahligen Function von $x, u_1, \ldots, u_m$ congruent; wir setzen ihn in die Gestalt

$$\Pi(x;\, u_1, \ldots, u_m) = x^f + V_1 x^{f-1} + \cdots + V_f,$$

wo $V_1, \ldots, V_f$ ganzzahlige Functionen von $u_1, \ldots, u_m$ bedeuten. Offenbar genügt die Fundamentalform ξ, für x gesetzt, der Congruenz

$$\Pi(x;\, u_1, \ldots, u_m) \equiv 0, \quad (\mathfrak{p}).$$

Da die Function $\Pi(x;\, a_1, \ldots, a_m) \equiv P(x)$ nach p ist, so folgt, dass auch $\mathfrak{p} = (p, \Pi(\varrho;\, a_1, \ldots, a_m))$ ist, und mithin sind die Coefficienten der Potenzen und Producte von $u_1, \ldots, u_m$ in $\Pi(\xi;\, u_1, \ldots, u_m)$ nicht sämtlich durch $\mathfrak{p}^2$ und auch nicht sämtlich durch ein von $\mathfrak{p}$ verschiedenes, in $\mathfrak{a}$ aufgehendes Primideal teilbar. Da $P(x)$ Primfunction ist, so gilt das Gleiche umsomehr von der Function $\Pi(x;\, u_1, \ldots, u_m)$.

Hülfssatz 4. Jede ganzzahlige Function $\Phi(x;\, u_1, \ldots, u_m)$, welche identisch in $u_1, \ldots, u_m$ nach $\mathfrak{p}$ dem Wert 0 congruent wird, sobald man für x die Fundamentalform ξ einsetzt, ist nach p durch $\Pi(x;\, u_1, \ldots, u_m)$ teilbar.

Beweis. Im gegenteiligen Falle hätten Φ und Π nach p keinen Teiler gemein, und es müsste folglich nach Satz 32 eine nach p dem Wert 0 nicht congruente ganzzahlige Function U von $u_1, \ldots, u_m$ allein existiren, so dass $U \equiv A\Phi + B\Pi$ nach p wird, wo A, B ganzzahlige Functionen von $x, u_1, \ldots, u_m$ sind. Hieraus würde, wenn man für x die Fundamentalform ξ einsetzt, $U \equiv 0$ nach $\mathfrak{p}$ und folglich auch nach p sich ergeben, was nicht der Fall ist.

Hülfssatz 5. Ist Φ eine ganzzahlige Function von $x, u_1, \ldots, u_m$, welche identisch in $u_1, \ldots, u_m$ nach $\mathfrak{p}^e$ dem Wert 0 congruent wird, wenn man für x die Fundamentalform ξ einsetzt, so muss notwendig Φ nach p durch Π^e teilbar sein.

Beweis. Setzen wir $\Phi \equiv \Pi^{e'} F$ nach p, wo $e' < e$ ist und F eine ganzzahlige Function von $x, u_1, \ldots, u_m$ bedeutet, die nach p nicht mehr durch Π teilbar ist, so folgt, dass sämtliche Coefficienten der Po-

tenzen und Producte von $u_1, \ldots, u_m$ in $\{\Pi(\xi; u_1, \ldots, u_m)\}^{e'} F(\xi; u_1, \ldots, u_m)$ durch $\mathfrak{p}^e$ teilbar sein müssen. Wir denken uns nun sowohl $\Pi(\xi; u_1, \ldots, u_m)$ als $F(\xi; u_1, \ldots, u_m)$ nach fallenden Potenzen der Variabeln u_1 und die Coefficienten der Potenzen von u_1 wiederum nach fallenden Potenzen von u_2 geordnet u. s. f. Ist dann π der erste Coefficient in $\Pi(\xi)$, welcher nicht durch $\mathfrak{p}^2$ teilbar ist, und zutreffendenfalls $\varkappa$ der erste Coefficient in $F(\xi)$, welcher nicht durch $\mathfrak{p}$ teilbar ist, so würde $\pi^{e'}\varkappa \equiv 0$ nach $\mathfrak{p}^e$ folgen, was nicht möglich ist; d. h. sämtliche Coefficienten von $F(\xi)$ sind durch $\mathfrak{p}$ teilbar, und hieraus folgt nach dem Hülfssatz 4, dass $F(x; u_1, \ldots, u_m)$ durch $\Pi(x; u_1, \ldots, u_m)$ nach p teilbar ist. Diese Folgerung widerspricht unserer Annahme.

§ 11.

Die Zerlegung der linken Seite der Fundamentalgleichung. Die Discriminante der Fundamentalgleichung.

Aus den Hülfssätzen 3, 4 und 5 folgen die nachstehenden wichtigen Thatsachen, welche die Zerlegung der linken Seite der Fundamentalgleichung betreffen:

Satz 33. Ist die Zerlegung der rationalen Primzahl p in Primideale durch die Formel $p = \mathfrak{p}^e \mathfrak{p}'^{e'} \ldots$ gegeben, so gestattet die linke Seite F der Fundamentalgleichung im Sinn der Congruenz nach p die Darstellung

$$F \equiv \Pi^e \Pi'^{e'} \ldots, \quad (p)$$

wo $\Pi, \Pi', \ldots$ gewisse verschiedene Primfunctionen von $x, u_1, \ldots, u_m$ nach p bedeuten; überdies ist, wenn

$$F = \Pi^e \Pi'^{e'} \cdots + p\,G$$

gesetzt wird, G eine ganzzahlige Function der Veränderlichen $x, u_1, \ldots, u_m$, welche nach p durch keine der Primfunctionen $\Pi, \Pi', \ldots$ teilbar ist.

Satz 34. Die aus der Fundamentalgleichung sich ergebende Congruenz $m$ten Grades

$$F(x; u_1, \ldots, u_m) \equiv 0, \quad (p)$$

ist zugleich die Congruenz niedrigsten Grades mit ganzen rationalen Coefficienten, welcher die Fundamentalform ξ, für x eingesetzt, nach p genügt.

Beweis. Es sei Φ eine ganzzahlige Function von $x, u_1, \ldots, u_m$ solcher Art, dass die Congruenz $\Phi(x) \equiv 0$ nach p von der Fundamentalform ξ befriedigt wird. Ferner seien die von einander verschiedenen, in p aufgehenden Primideale $\mathfrak{p}, \mathfrak{p}', \ldots$ bezüglich von den Graden $f, f', \ldots$; durch Bildung der Norm folgt $p^m = p^{fe+f'e'+\cdots}$, d. h. $m = fe + f'e' + \cdots$.

Ferner mögen Π, Π', ... bez. die zu den Primidealen $\mathfrak{p}$, $\mathfrak{p}'$, ... gehörigen Primfunctionen von x, u_1, ..., u_m bedeuten, wie sie in den vorigen Hülfssätzen gebraucht worden sind. Aus dem Hülfssatz 5 folgt dann

$$\Phi \equiv \Pi^e \Pi'^{e'} \ldots \Psi, \quad (p)$$

wo Ψ eine ganzzahlige Function bezeichnet. Da Π, Π', ... bezüglich von der Graden f, f', ... in x sind, so folgt, dass Φ mindestens vom $m$ten Grade in x sein muss, und dieser Umstand liefert, wenn man an Stelle von Φ die linke Seite F der Fundamentalgleichung wählt, den ersten Teil des Satzes 33 und den Satz 34.

Wäre endlich $G(x)$ nach p etwa durch $\Pi(x)$ teilbar, so würde die Fundamentalform ξ, für x eingesetzt, der Congruenz $G(x) \equiv 0$ nach $\mathfrak{p}$ und folglich auch der Congruenz $\Pi^e(x) \Pi'^{e'}(x) \cdots \equiv 0$ nach $\mathfrak{p}^{e+1}$ genügen müssen, was nach Hülfssatz 5 nicht möglich ist. Damit ist auch der zweite Teil des Satzes 33 bewiesen.

Die gefundenen Thatsachen bedingen eine Reihe von wichtigen Discriminantensätzen:

Satz 35. Der grösste Zahlenfactor von der Discriminante der Fundamentalgleichung ist gleich der Discriminante des Körpers.

Beweis. Wir setzen

$$(2.) \quad \begin{cases} 1 = U_{11}\,\omega_1 + \cdots + U_{1m}\,\omega_m, \\ \xi = U_{21}\,\omega_1 + \cdots + U_{2m}\,\omega_m, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \xi^{m-1} = U_{m1}\,\omega_1 + \cdots + U_{mm}\,\omega_m, \end{cases}$$

wo U_{11}, ..., U_{mm} ganzzahlige Functionen von u_1, ..., u_m seien. Wäre nun die Determinante U dieser m^2 Functionen eine solche Function, deren sämtliche Coefficienten etwa durch die rationale Primzahl p teilbar sind, so gäbe es offenbar m nicht sämtlich dem Werte 0 nach p congruente ganzzahlige Functionen V_1, ..., V_m von u_1, ..., u_m der Art, dass identisch in u_1, ..., u_m

$$V_1 U_{11} + \cdots + V_m U_{m1} \equiv 0, \quad (p)$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$
$$V_1 U_{1m} + \cdots + V_m U_{mm} \equiv 0, \quad (p)$$

wird. Mithin müsste die Fundamentalform ξ der Congruenz

$$V_1 + V_2 \xi + \cdots + V_m \xi^{m-1} \equiv 0, \quad (p)$$

genügen, welche von niederem als $m$tem Grade ist. Da dies nach Satz 34

nicht statthaben kann, so folgt, dass die Determinante U eine rationale Einheitsform ist.

Die Gleichungen (2.) ergeben mit Hülfe des Multiplicationssatzes der Determinanten:

$$\begin{vmatrix} 1, & \xi, & \ldots, & \xi^{m-1} \\ 1, & \xi', & \ldots, & \xi'^{m-1}, \\ \cdot & \cdot & \cdot & \cdot \\ 1, & \xi^{(m-1)}, & \ldots, & (\xi^{(m-1)})^{m-1} \end{vmatrix} = U \begin{vmatrix} \omega_1, & \ldots, & \omega_m \\ \omega_1', & \ldots, & \omega_m' \\ \cdot & \cdot & \cdot \\ \omega_1^{(m-1)}, & \ldots, & \omega_m^{(m-1)} \end{vmatrix}.$$

Durch Quadriren dieser Beziehung folgt $d(\xi) = U^2 d$ oder $d(\xi) \simeq d$, wo $d(\xi)$ die Discriminante der Fundamentalgleichung und d die Körperdiscriminante bedeutet.

Durch Auflösung der Gleichungen (2) ergiebt sich ferner die folgende Thatsache:

Satz 36. Jede ganze Zahl des Körpers k ist gleich einer ganzen rationalen Function $(m-1)$ten Grades der Fundamentalform ξ, und zwar sind die Coefficienten dieser Function ganzzahlige Functionen von $u_1, \ldots, u_m$, dividirt durch die rationale Einheitsform U. [*Kronecker*[16], *Hensel*[4].]

§ 12.

Die Elemente und die Differente des Körpers. Beweis des Satzes über die Teiler der Körperdiscriminante.

Der Satz 35 gestattet die Zerlegung der Körperdiscriminante d in gewisse ideale Factoren. Die $m-1$ Ideale

$$\begin{aligned} \mathfrak{e}' &= ((\omega_1 - \omega_1'), \quad \ldots, \quad (\omega_m - \omega_m')), \\ \mathfrak{e}'' &= ((\omega_1 - \omega_1''), \quad \ldots, \quad (\omega_m - \omega_m'')), \\ &\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \mathfrak{e}^{(m-1)} &= ((\omega_1 - \omega_1^{(m-1)}), \quad \ldots, \quad (\omega_m - \omega_m^{(m-1)})) \end{aligned}$$

nenne ich die $m-1$ **Elemente** des Körpers k. Dieselben sind Ideale, welche im allgemeinen dem Zahlkörper k nicht angehören; dagegen ist das Product $\mathfrak{d} = \mathfrak{e}'\mathfrak{e}''\ldots\mathfrak{e}^{(m-1)}$ ein Ideal des Körpers k. Bedenken wir nämlich, dass die Elemente $\mathfrak{e}', \ldots, \mathfrak{e}^{(m-1)}$ bez. die Inhalte der Formen $\xi - \xi', \ldots, \xi - \xi^{(m-1)}$ sind, so erkennen wir nach Satz 13, dass das Ideal $\mathfrak{d}$ den Inhalt von der Differente der Fundamentalform, nämlich von

$$\frac{\partial F}{\partial \xi} = (\xi - \xi')\ldots(\xi - \xi^{(m-1)})$$

bildet, und diese ist eine Form des Körpers k. Das Ideal $\mathfrak{d}$ nenne ich die **Differente***) **des Körpers.** Die Norm derselben ist gleich dem grössten Zahlenfactor von der Discriminante der Fundamentalform, und, da dieser nach Satz 35 gleich d ist, so folgt der Satz:

Satz 37. Die Norm der Differente des Körpers ist gleich der Discriminante des Körpers.

Aus der Congruenz

$$\frac{\partial F(x)}{\partial x} \equiv e\Pi^{e-1}\frac{\partial \Pi}{\partial x}\Pi'^{e'}\cdots + e'\Pi^{e}\Pi'^{e'-1}\frac{\partial \Pi'}{\partial x}\cdots + \cdots, \quad (p)$$

folgt ferner, dass die Differente des Körpers stets durch $\mathfrak{p}^{e-1}$ teilbar ist, und dass sie jedenfalls dann keine höhere Potenz von $\mathfrak{p}$ enthält, sobald der Exponent e zu p prim ist. Durch Uebergang zur Norm ergiebt sich hieraus, dass die Discriminante des Körpers stets durch $p^{f(e-1)+f'(e'-1)+\cdots}$ teilbar ist und überdies jedenfalls dann keine höhere Potenz von p enthält, wenn sämtliche Exponenten $e, e', \ldots$ zu p prim sind; damit ist zugleich der am Anfang des § 10 aufgestellte Fundamentalsatz 31 bewiesen.

§ 13.

Die Aufstellung der Primideale. Der feste Zahlteiler der rationalen Einheitsform U.

Die wirkliche Berechnung der in einer rationalen Primzahl p aufgehenden Primideale kann auf Grund des Satzes 33 durch Zerlegung der linken Seite der Fundamentalgleichung ausgeführt werden. Doch ist es von Nutzen zu wissen, unter welchen Umständen hierbei den Parametern $u_1, \ldots, u_m$ in der Fundamentalgleichung specielle Werte beigelegt werden dürfen. Wir stellen zu dem Zweck die folgenden Betrachtungen an.

Die Discriminanten aller ganzen algebraischen Zahlen des Körpers erhält man, wenn man in $U^2 d$ die Parameter $u_1, \ldots, u_m$ alle ganzen rationalen Zahlen durchlaufen lässt. Der grösste gemeinsame Teiler aller dieser Discriminanten braucht nicht mit der Körperdiscriminante d übereinzustimmen, da sehr wohl der Fall eintreten kann, dass die rationale Einheitsform U für alle ganzzahligen Werte der $u_1, \ldots, u_m$ eine Reihe von Zahlen mit einem festen Teiler $\neq 1$ darstellt. Dieser Umstand setzt die Bedeutung des Gebrauchs der Unbestimmten $u_1, \ldots, u_m$ in helles Licht. Man findet auch leicht eine notwendige und hinreichende Bedingung da-

*) Nach *Dedekind* „das Grundideal".

für, dass die rationale Primzahl p ein solcher fester Teiler von U ist. Diese Bedingung besteht nämlich darin, dass U in die Gestalt

$$p\,V + (u_1^p - u_1)\,V_1 + \cdots + (u_m^p - u_m)\,V_m$$

gebracht werden kann, wo $V, V_1, \ldots, V_m$ ganzzahlige Functionen von $u_1, \ldots, u_m$ sind. [*Hensel*[1,2,5].]

Wenn es nun möglich ist, den Unbestimmten $u_1, \ldots, u_m$ solche ganzen rationalen Zahlenwerte $a_1, \ldots, a_m$ zu erteilen, dass für dieselben die rationale Einheitsform U eine durch p nicht teilbare Zahl wird, so darf bei der Zerlegung der rationalen Primzahl p die Fundamentalgleichung so specialisirt werden, dass die Form ξ durch $\alpha = a_1\omega_1 + \cdots + a_m\omega_m$ ersetzt wird. In der That, unter der gemachten Annahme ist, wie leicht aus Satz 36 folgt, jede beliebige ganze Zahl ω des Körpers einer ganzzahligen Function von α nach p congruent, und es ist daher eine ganzzahlige Function von niederem als $m$tem Grade in α niemals durch p teilbar, wenn nicht ihre Coefficienten sämtlich durch p teilbar sind. Bezeichnen wir die aus $\Pi(x;\, u_1, \ldots, u_m)$, $\Pi'(x;\, u_1, \ldots, u_m)$, ... durch die Substitution $u_1 = a_1, \ldots, u_m = a_m$ hervorgehenden Functionen von x allein mit $P(x)$, $P'(x)$, ..., so erkennen wir, dass diese Functionen im Sinne der Congruenz nach p von einander verschiedene Primfunctionen sind, und dass

$$\mathfrak{p} = (p,\, P(\alpha)), \quad \mathfrak{p}' = (p,\, P'(\alpha)), \quad \ldots$$

wird. In der That, würde etwa $P(\alpha)$ nach Forthebung des Factors $\mathfrak{p}$ noch einen in p aufgehenden Primfactor, z. B. $\mathfrak{p}'$, enthalten, so wäre

$$\{P(\alpha)\}^{e}\{P'(\alpha)\}^{e'-1}\{P''(\alpha)\}^{e''}\cdots \equiv 0, \quad (p)$$

was nach obiger Bemerkung nicht der Fall sein kann, da die linke Seite dieser Congruenz eine Function von niederem als $m$tem Grade in α darstellt.

Umgekehrt gilt die leicht zu beweisende Thatsache: Wenn im Körper k die Zerlegung $p = \mathfrak{p}^{e}\mathfrak{p}'^{e'}\ldots$ gilt, wo $\mathfrak{p}, \mathfrak{p}', \ldots$ von einander verschiedene Primideale bezüglich von den Graden $f, f', \ldots$ sind, und wenn man dann diesen Primidealen $\mathfrak{p}, \mathfrak{p}', \ldots$ ebenso viele ganzzahlige Functionen $P(x)$, $P'(x)$, ... der einen Veränderlichen x zuordnen kann, die im Sinne der Congruenz nach p Primfunctionen bez. von den Graden $f, f', \ldots$ und unter einander verschieden sind, so lässt sich stets eine Zahl $\alpha = a_1\omega_1 + \cdots + a_m\omega_m$ finden, für welche der zugehörige Wert von U nicht durch p teilbar ist. Die Nichtexistenz solcher von einander verschiedener Primfunctionen $P(x)$, $P'(x)$, ... im Sinne der Congruenz nach

der rationalen Primzahl p bildet daher eine neue notwendige und hinreichende Bedingung dafür, dass die Primzahl p als fester Zahlteiler in U auftritt. [*Dedekind*[4].]

Jede der beiden in diesem Paragraphen gefundenen, wesentlich von einander verschiedenen Bedingungen kann zur Berechnung numerischer Beispiele für Zahlkörper dienen, in deren U wirklich feste Zahlteiler $\neq 1$ der fraglichen Weise enthalten sind. [*Dedekind*[4], *Kronecker*[16], *Hensel*[1, 2, 5].]

Es ist jedoch zu bemerken, dass die Form U die Eigenschaft, feste Zahlteiler zu enthalten, verliert, wenn man in derselben die Unbestimmten $u_1, \ldots, u_m$ alle ganzen algebraischen Zahlen eines geeignet gewählten Zahlkörpers durchlaufen lässt, indem die sämtlichen durch U auf diese Art darstellbaren Zahlen den grössten gemeinsamen Teiler 1 erhalten. [*Hensel*[5].]

Capitel V.

Der Relativkörper.

§ 14.

Die Relativnorm, die Relativdifferente und die Relativdiscriminante.

Die Begriffe Norm, Differente und Discriminante sind einer wichtigen Verallgemeinerung fähig.

Ist K ein Körper vom Grade M, welcher sämtliche Zahlen des Körpers k vom $m$ten Grade enthält, so heisst k ein **Unterkörper** von K. Der Körper K wird der **Oberkörper** von k oder der **Relativkörper** in Bezug auf k genannt. Es sei Θ eine den Körper K bestimmende Zahl. Unter den unendlich vielen Gleichungen mit algebraischen, in k liegenden Coefficienten, denen die Zahl Θ genügt, habe die folgende Gleichung vom Grade r

$$\Theta^r + \alpha_1 \Theta^{r-1} + \cdots + \alpha_r = 0 \tag{3.}$$

den niedrigsten Grad; $\alpha_1, \ldots, \alpha_r$ sind dann bestimmte Zahlen in k. Der Grad r heisst der **Relativgrad** des Körpers K in Bezug auf k; es ist $M = rm$. Die Gleichung (3) vom $r$ten Grade ist im Rationalitätsbereich k irreducibel. Sind $\Theta', \ldots, \Theta^{(r-1)}$ die $r-1$ anderen Wurzeln der Gleichung (3.), so heissen diese $r-1$ algebraischen Zahlen die **zu Θ relativ conjugirten Zahlen,** und die bez. durch $\Theta', \ldots, \Theta^{(r-1)}$ bestimmten Körper $K', \ldots, K^{(r-1)}$ heissen die zu K **relativ con-**

jugirten Körper. Ist A eine beliebige Zahl des Körpers K, und ist

$$A = \gamma_1 + \gamma_2 \Theta + \cdots + \gamma_r \Theta^{r-1},$$

wo $\gamma_1, \gamma_2, \ldots, \gamma_r$ Zahlen in k sind, so heissen die Zahlen

$$A' = \gamma_1 + \gamma_2 \Theta' + \cdots + \gamma_r \Theta'^{r-1},$$
$$\cdots\cdots\cdots\cdots$$
$$A^{(r-1)} = \gamma_1 + \gamma_2 \Theta^{(r-1)} + \cdots + \gamma_r (\Theta^{(r-1)})^{r-1}$$

die bez. durch die Substitutionen $T' = (\Theta : \Theta'), \ldots, T^{(r-1)} = (\Theta : \Theta^{(r-1)})$ aus A entspringenden oder **zu A relativ conjugirten Zahlen.** Wendet man auf die sämtlichen Zahlen eines Ideals $\mathfrak{J}$ die Substitution T' an, so heisst das dann entstehende Ideal $\mathfrak{J}'$ das durch T' aus $\mathfrak{J}$ entspringende oder **zu $\mathfrak{J}$ relativ conjugirte Ideal.**

Wenn $\alpha_1, \ldots, \alpha_s$ beliebige Zahlen in k sind und $\mathfrak{j} = (\alpha_1, \ldots, \alpha_s)$ das durch sie bestimmte Ideal in k bezeichnet, so wird durch die nämlichen Zahlen auch zugleich ein Ideal $\mathfrak{J} = (\alpha_1, \ldots, \alpha_s)$ im Körper K bestimmt. Dieses Ideal $\mathfrak{J}$ ist als nicht verschieden von $\mathfrak{j}$ anzusehen. Ein Ideal $\mathfrak{J} = (A_1, \ldots, A_S)$ des Körpers K wird umgekehrt dann und nur dann auch als ein Ideal $\mathfrak{j}$ des Körpers k bezeichnet, wenn $\mathfrak{J}$ sich zugleich als grösster gemeinsamer Teiler von gewissen ganzen Zahlen $\alpha_1, \ldots, \alpha_s$ des Körpers k darstellen lässt. Das Product einer Zahl A mit den relativ conjugirten Zahlen

$$N_k(A) = A A' \ldots A^{(r-1)}$$

heisst die **Relativnorm der Zahl** A bezüglich des Körpers oder Rationalitätsbereiches k. Die Relativnorm N_k ist eine Zahl in k. Ist $\mathfrak{J} = (A_1, \ldots, A_S)$ ein beliebiges Ideal in K, so heisst das Product von $\mathfrak{J}$ mit den sämtlichen relativ conjugirten Idealen von $\mathfrak{J}$

$$N_k(\mathfrak{J}) = \mathfrak{J}\mathfrak{J}' \ldots \mathfrak{J}^{(r-1)}$$

die **Relativnorm des Ideals** $\mathfrak{J}$. Die Relativnorm $N_k(\mathfrak{J})$ ist ein Ideal des Körpers k. Bedeuten nämlich $U_1, \ldots, U_S$ Unbestimmte, so sind die Coefficienten des Ausdruckes

$$(A_1 U_1 + \cdots + A_S U_S)(A_1' U_1 + \cdots + A_S' U_S) \ldots (A_1^{(r-1)} U_1 + \cdots + A_S^{(r-1)} U_S)$$

ganze Zahlen in k, deren grösster gemeinsamer Teiler nach Satz 13 mit jenem Idealproducte übereinstimmen muss.

Der Ausdruck

$$\Delta_k(A) = (A - A')(A - A'') \ldots (A - A^{(r-1)})$$

stellt eine Zahl des Körpers K dar und heisst die **Relativdifferente**

der Zahl A in Bezug auf den Körper k. Der Ausdruck

$$D_k(A) = (A-A')^2(A-A'')^2\ldots(A^{(r-2)}-A^{(r-1)})^2$$

heisst die **Relativdiscriminante der Zahl** A. Dieselbe ist bis auf das Vorzeichen gleich der Relativnorm der Relativdifferente von A; es ist nämlich $D_k(A) = (-1)^{\frac{r(r-1)}{2}} N_k(\varDelta_k)$.

Sind $\Omega_1, \ldots, \Omega_M$ die M Basiszahlen des Körpers K, so heisst das durch Multiplication der $r-1$ Elemente

$$\begin{array}{lll} \mathfrak{E}' & = ((\Omega_1-\Omega_1'), & \ldots, \quad (\Omega_M-\Omega_M')), \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \mathfrak{E}^{(r-1)} & = ((\Omega_1-\Omega_1^{(r-1)}), & \ldots, \quad (\Omega_M-\Omega_M^{(r-1)})) \end{array}$$

entstehende Ideal

$$\mathfrak{D}_k = \mathfrak{E}'\mathfrak{E}''\ldots\mathfrak{E}^{(r-1)}$$

die Relativdifferente des Körpers K in Bezug auf k. Bezeichnet

$$\varXi = \Omega_1 U_1 + \cdots + \Omega_M U_M$$

die Fundamentalform von K, so ist die Relativdifferente von $\varXi$

$$\varDelta_k(\varXi) = (\varXi-\varXi')\ldots(\varXi-\varXi^{(r-1)}).$$

Die Coefficienten dieser Form sind Zahlen des Körpers K, und da nach dem Satze 13 der grösste gemeinsame Teiler derselben die Relativdifferente $\mathfrak{D}_k$ ergeben muss, so ist $\mathfrak{D}_k$ ein Ideal des Körpers K.

Das Quadrat des grössten gemeinsamen Teilers aller r-reihigen Determinanten der Matrix

$$(4.) \qquad \begin{vmatrix} \Omega_1, & \Omega_2, & \ldots, & \Omega_M \\ \Omega_1', & \Omega_2', & \ldots, & \Omega_M' \\ \cdot & \cdot & \cdot & \cdot \\ \Omega_1^{(r-1)}, & \Omega_2^{(r-1)}, & \ldots, & \Omega_M^{(r-1)} \end{vmatrix}$$

heisst die **Relativdiscriminante** D_k **des Körpers** K bez. k; dieselbe ist, wie leicht ersichtlich, ein Ideal des Körpers k.

§ 15.

Eigenschaften der Relativdifferente und der Relativdiscriminante eines Körpers.

Hinsichtlich der soeben definirten Begriffe gelten folgende Sätze: [*Hilbert*[3].]

Satz 38. Die Relativdiscriminante des Körpers K in Bezug auf den Unterkörper k ist gleich der Relativnorm der Relativdifferente von K, d. h.

$$D_k = N_k(\mathfrak{D}_k).$$

Beweis. Die Relativnorm von der Relativdifferente der Fundamentalform Ξ ist

$$N_k(\varDelta_k(\Xi)) = \pm(\Xi-\Xi')^2(\Xi-\Xi'')^2\dots(\Xi^{(r-2)}-\Xi^{(r-1)})^2$$

$$= \pm\begin{vmatrix} 1, & \Xi, & \dots, & \Xi^{r-1} \\ 1, & \Xi', & \dots, & (\Xi')^{r-1} \\ \cdot & \cdot & \cdot & \cdot \\ 1, & \Xi^{(r-1)}, & \dots, & (\Xi^{(r-1)})^{r-1} \end{vmatrix}^2.$$

Andererseits ist das rechtsstehende Determinantenquadrat eine Form des Körpers K, deren Inhalt gleich der Relativdiscriminante D_k ist. Drücken wir nämlich die Terme der obigen Determinante linear durch $\Omega_1, \dots, \Omega_M$ bezüglich durch die conjugirten Basiszahlen des Körpers K aus, wobei die Coefficienten in diesen Ausdrücken ganzzahlige Functionen von $U_1, \dots, U_M$ sind, so erkennen wir, dass jenes Determinantenquadrat lauter durch D_k teilbare Coefficienten besitzt. Umgekehrt zeigt eine Uebertragung des Satzes 36, dass eine jede r-reihige Determinante der Matrix (4.) nach Multiplication mit der $r$ten Potenz einer gewissen in den Parametern $U_1, \dots, U_M$ geschriebenen rationalen Einheitsform durch das Differenzenproduct

$$(\Xi-\Xi')(\Xi-\Xi'')\dots(\Xi^{(r-2)}-\Xi^{(r-1)})$$

teilbar wird. Daraus folgt $N_k(\varDelta_k(\Xi)) \simeq D_k$.

Satz 39. Bedeuten D und d die Discriminanten des Oberkörpers K und des Unterkörpers k und bezeichnet $n(D_k)$ die Norm der Relativdiscriminante D_k, genommen im Körper k, so ist

$$D = d^r n(D_k).$$

Beweis. Ist $\xi = \omega_1 u_1 + \dots + \omega_m u_m$ die Fundamentalform des Körpers k, so genügt Ξ, für X gesetzt, einer Gleichung $r$ten Grades in X von der Gestalt

$$\Phi(X, \xi) = \Phi_0 X^r + \Phi_1 X^{r-1} + \dots + \Phi_r = 0,$$

wo $\Phi_1, \dots, \Phi_r$ ganzzahlige Functionen von ξ und den Unbestimmten $u_1, \dots, u_m, U_1, \dots, U_M$ sind, und wo Φ_0 eine rationale Einheitsform der Unbestimmten $u_1, \dots, u_m$ ist. Die übrigen Wurzeln der obigen Gleichung $r$ten Grades sind $X = \Xi', \dots, \Xi^{(r-1)}$. Sodann sei $\xi^{(h)}$ eine der $m-1$ zu ξ conjugirten Fundamentalformen; die Wurzeln der Gleichung $r$ten Grades $\Phi(X, \xi^{(h)}) = 0$ mögen mit $\Xi_{(h)}, \Xi'_{(h)}, \dots, \Xi^{(r-1)}_{(h)}$ bezeichnet werden. Da nun ξ einer Gleichung $m$ten Grades genügt, so ist offenbar jede Potenz von Ξ nach Multiplication mit einer Potenz von Φ_0 gleich einer ganzen Function von ξ und Ξ, welche in ξ höchstens

bis zum Grade $m-1$ und in Ξ höchstens bis zum Grade $r-1$ ansteigt, und deren Coefficienten ganzzahlige Functionen der Parameter $u_1, \ldots, u_m$, $U_1, \ldots, U_M$ sind. Infolge dessen ist notwendigerweise die Discriminante der Fundamentalform Ξ nach Multiplication mit einer Potenz von Φ_0 durch das Quadrat der $M = rm$-reihigen Determinante

$$\varDelta = \begin{vmatrix} 1, & \Xi, & \ldots, & \Xi^{r-1}, & \xi, & \xi\Xi, & \ldots, & \xi\Xi^{r-1}, & \ldots \\ & & \ldots, & \xi^{m-1}, & \xi^{m-1}\Xi, & & \ldots, & \xi^{m-1}\Xi^{r-1} & \\ 1, & \Xi', & \ldots, & \Xi'^{r-1}, & \xi, & \xi\Xi', & \ldots, & \xi\Xi'^{r-1}, & \ldots \\ & & \ldots, & \xi^{m-1}, & \xi^{m-1}\Xi', & & \ldots, & \xi^{m-1}\Xi'^{r-1} & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1, & \Xi^{r-1}, & \ldots, & (\Xi^{(r-1)})^{r-1}, & \xi, & \xi\Xi^{(r-1)}, & \ldots, & \xi(\Xi^{(r-1)})^{r-1}, & \ldots \\ & & \ldots, & \xi^{m-1}, & \xi^{m-1}\Xi^{r-1}, & & \ldots, & \xi^{m-1}(\Xi^{(r-1)})^{r-1} & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix}$$

teilbar; hierbei sind in dem Schema nur die ersten r Horizontalreihen hingeschrieben; die übrigen $r(m-1)$ Horizontalreihen entstehen, wenn man der Reihe nach allen Buchstaben ξ die Zeichen $(h) = (1), \ldots, (m-1)$ als obere Indices und zugleich allen Buchstaben Ξ die nämlichen Zeichen als untere Indices anfügt.

Drückt man nun die Elemente der Determinante $\varDelta$ linear durch die Basiszahlen $\Omega_1, \ldots, \Omega_M$ und deren Conjugirte aus, so erkennen wir die Richtigkeit der Formel

$$\varDelta = \begin{vmatrix} \Omega_1, & \ldots, & \Omega_M \\ \Omega_1', & \ldots, & \Omega_M' \\ \cdot & \cdot & \cdot \\ \Omega_1^{(M-1)}, & \ldots, & \Omega_M^{(M-1)} \end{vmatrix} F,$$

wo F eine ganzzahlige Function der Parameter $u_1, \ldots, u_m$, $U_1, \ldots, U_M$ bedeutet. Hieraus folgt, dass der Zahlenfactor des Quadrates von $\varDelta$ durch D teilbar ist. Da aber der Zahlenfactor der Discriminante von Ξ nach Satz 35 $= D$ wird, so folgt aus obiger Entwickelung, dass auch umgekehrt D durch den Zahlenfactor des Quadrates von $\varDelta$ teibar ist; d. h. der Zahlenfactor von $\varDelta^2$ ist gleich D.

Aus elementaren Sätzen der Determinantentheorie ergiebt sich nun die Identität

$$\varDelta = \begin{vmatrix} 1, & \xi, & \ldots, & \xi^{m-1} \\ 1, & \xi', & \ldots, & \xi'^{m-1} \\ \cdot & \cdot & \cdot & \cdot \\ 1, & \xi^{(m-1)}, & \ldots, & (\xi^{(m-1)})^{m-1} \end{vmatrix}^r \Pi,$$

wo

$$\Pi = \begin{vmatrix} 1, & \Xi, & \ldots, & \Xi^{r-1} \\ 1, & \Xi', & \ldots, & \Xi'^{r-1} \\ \cdot & \cdot & \cdot & \cdot \\ 1, & \Xi^{(r-1)}, & \ldots, & (\Xi^{(r-1)})^{r-1} \end{vmatrix} \begin{vmatrix} 1, & \Xi_{(1)}, & \ldots, & \Xi_{(1)}^{r-1} \\ 1, & \Xi'_{(1)}, & \ldots, & \Xi'^{r-1}_{(1)} \\ \cdot & \cdot & \cdot & \cdot \\ 1, & \Xi_{(1)}^{(r-1)}, & \ldots, & (\Xi_{(1)}^{(r-1)})^{r-1} \end{vmatrix} \cdots$$

$$\cdots \begin{vmatrix} 1, & \Xi_{(m-1)}, & \ldots, & \Xi_{(m-1)}^{r-1} \\ 1, & \Xi'_{(m-1)}, & \ldots, & \Xi'^{r-1}_{(m-1} \\ \cdot & \cdot & \cdot & \cdot \\ 1, & \Xi_{(m-1)}^{(r-1)}, & \ldots, & (\Xi_{(m-1)}^{(r-1)})^{r-1} \end{vmatrix}$$

gesetzt ist, und hieraus folgt unmittelbar der Satz 39.

Der eben bewiesene Satz 39 zeigt nicht nur, dass die Discriminante eines Körpers durch die Discriminante eines jeden Unterkörpers teilbar ist, sondern giebt eine gewisse Potenz der letzteren an, welche in der Discriminante des Oberkörpers aufgeht, und deckt auch zugleich die einfache Bedeutung des übrig bleibenden Factors der Discriminante des Oberkörpers auf.

§ 16.

Die Zerlegung eines Elementes des Körpers k im Oberkörper K. Der Satz von der Differente des Oberkörpers K.

Satz 40. *Jedes Element des Unterkörpers k ist dem Product von gewissen r Elementen des Oberkörpers K gleich, und zwar gelten die Formeln:*

$$\xi - \xi^{(h)} \cong (\Xi - \Xi_{(h)})(\Xi - \Xi'_{(h)}) \ldots (\Xi - \Xi_{(h)}^{(r-1)})$$
$$\cong (\Xi - \Xi_{(h)})(\Xi' - \Xi_{(h)}) \ldots (\Xi^{(r-1)} - \Xi_{(h)}).$$

Beweis. Ist

$$F(X) = X^M + F_1 X^{M-1} + \cdots + F_M = 0$$

die Fundamentalgleichung Mten Grades des Körpers K, wobei $F_1, \ldots, F_M$ ganzzahlige Functionen von $U_1, \ldots, U_M$ bedeuten, so gilt identisch in X die Gleichung

$$\Phi_0^m F(X) = \Phi(X, \xi)\Phi(X, \xi')\ldots\Phi(X, \xi^{(m-1)}).$$

Die Differente der Fundamentalform Ξ ist mithin wegen $\Phi(\Xi, \xi) = 0$ durch die Formel

$$\Delta(\Xi) = \frac{\partial F(\Xi)}{\partial \Xi} = \frac{1}{\Phi_0^m} \frac{\partial \Phi(\Xi, \xi)}{\partial \Xi} \Phi(\Xi, \xi')\ldots\Phi(\Xi, \xi^{(m-1)})$$

dargestellt. Nun ist einerseits

$$(5.)\quad \Phi(\Xi,\ \xi^{(h)}) = \Phi_0(\Xi - \Xi_{(h)})(\Xi - \Xi'_{(h)})\dots(\Xi - \Xi^{(r-1)}_{(h)}),$$
$$(h = 1, 2, \dots, m-1)$$

und andererseits ist

$$(6.)\quad \Phi(\Xi,\ \xi^{(h)}) = \Phi(\Xi,\ \xi^{(h)}) - \Phi(\Xi,\ \xi) = (\xi - \xi^{(h)})\,G^{(h)},$$

wo $G^{(h)}$ eine ganze algebraische Form bedeutet; aus diesen Formeln folgt:

$$\Phi_0^m \frac{\partial F(\Xi)}{\partial \Xi} = \frac{\partial \Phi(\Xi,\ \xi)}{\partial \Xi}(\xi - \xi')\dots(\xi - \xi^{(m-1)})\,G'\dots G^{(m-1)}.$$

Da $\dfrac{1}{\Phi_0}\dfrac{\partial \Phi(\Xi,\ \xi)}{\partial \Xi}$ die Relativdifferente von Ξ darstellt, so folgt nach Satz 13 aus der letzten Formel

$$(7.)\qquad \mathfrak{D} = \mathfrak{D}_k \mathfrak{d} \mathfrak{J},$$

wo $\mathfrak{D}$ die Differente von K, $\mathfrak{D}_k$ die Relativdifferente von K in Bezug auf k, und wo $\mathfrak{J}$ dasjenige Ideal bedeutet, welches den Inhalt der Form $G'\dots G^{(m-1)}$ ausmacht. Durch Normbildung ergiebt sich $D = n(D_k)\,d^r N(\mathfrak{J})$, und folglich ist nach Satz 39 $N(\mathfrak{J}) = 1$, d. h. $\mathfrak{J} = 1$. Die Formen $G', \dots, G^{(m-1)}$ sind daher sämtlich Einheitsformen, und die Formeln (5) und (6) beweisen unseren Satz 40.

Der Satz 40 liefert die Zerlegung der Elemente des Körpers k im Oberkörper K; er ist das Fundament der Theorie der Discriminanten. Die Formel (7) liefert überdies die wichtige Thatsache:

Satz 41. Die Differente $\mathfrak{D}$ des Körpers K ist gleich dem Product der Relativdifferente $\mathfrak{D}_k$ von K in Bezug auf den Unterkörper k und der Differente $\mathfrak{d}$ des Körpers k, d. h. es ist

$$\mathfrak{D} = \mathfrak{D}_k \mathfrak{d}.$$

Nach diesem Satze ist das Verhalten der Differenten beim Uebergange von dem Unterkörper in den Oberkörper von merkwürdiger Einfachheit: man bekommt die Differente des höheren Körpers, indem man die Differente des niederen Körpers mit der betreffenden Relativdifferente multiplicirt.

Capitel VI.

Die Einheiten des Körpers.

§ 17.

Die Existenz conjugirter Zahlen, deren absolute Beträge gewissen Ungleichungen genügen.

Nachdem in Capitel II die Teilbarkeitsgesetze der Zahlen eines algebraischen Körpers ausführlich behandelt sind, gehen wir dazu über, diejenigen Wahrheiten zu entwickeln, bei deren Ergründung der Grössenbegriff eine wesentliche Rolle spielt. Das wichtigste Hülfsmittel bei diesen Untersuchungen bildet der folgende Satz: [*Minkowski* [3]]

Hülfssatz 6. Sind

$$f_1 = a_{11} u_1 + \cdots + a_{1m} u_m,$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$
$$f_m = a_{m1} u_1 + \cdots + a_{mm} u_m$$

m lineare homogene Formen von $u_1, \ldots, u_m$ mit beliebigen reellen Coefficienten $a_{11}, \ldots, a_{mm}$ und der Determinante 1, so kann man $u_1, \ldots, u_m$ stets als ganze rationale Zahlen, die nicht sämtlich 0 sind, so bestimmen, dass die Werte jener m Formen $f_1, \ldots, f_m$, absolut genommen, sämtlich $\leqq 1$ werden.

Dieser Satz erhält durch eine leichte Umformung die Gestalt:

Hülfssatz 7. Sind $f_1, \ldots, f_m$ m lineare homogene Formen von $u_1, \ldots, u_m$ mit beliebigen reellen Coefficienten und der positiven Determinante A, und bedeuten $\varkappa_1, \ldots, \varkappa_m$ beliebige positive Constante, deren Product gleich A ist, so kann man $u_1, \ldots, u_m$ stets als ganze rationale Zahlen, die nicht sämtlich 0 sind, so bestimmen, dass die absoluten Werte jener m Formen den Bedingungen

$$|f_1| \leqq \varkappa_1, \quad \ldots, \quad |f_m| \leqq \varkappa_m$$

genügen.

Es sei bemerkt, dass in diesem Capitel, abweichend von dem Früheren, der Körper k und die $m-1$ zu k conjugirten Körper bezüglich mit $k = k^{(1)}, k^{(2)}, \ldots, k^{(m)}$ und dem entsprechend allgemein die in $k^{(s)}$ liegenden, zu $\omega_1, \ldots, \omega_m$ conjugirten Basiszahlen mit $\omega_1^{(s)}, \ldots, \omega_m^{(s)}$ bezeichnet werden.

Den Hülfssatz 7 verwenden wir zum Beweise der folgenden Thatsache:

Satz 42. Sind $\varkappa_1, \ldots, \varkappa_m$ beliebige reelle positive Constante,

deren Product gleich $|\sqrt{d}|$ ist, und die den Bedingungen $\varkappa_s = \varkappa_{s'}$ genügen, falls $k^{(s)}$ und $k^{(s')}$ conjugirt imaginäre Körper sind, so giebt es im Körper k immer eine ganze von 0 verschiedene Zahl ω so, dass

$$|\omega^{(1)}| \leqq \varkappa_1, \quad . \;.\; ., \quad |\omega^{(m)}| \leqq \varkappa_m$$

wird.

Beweis. Wir ordnen den Körpern $k^{(1)}, \ldots, k^{(m)}$ gewisse Linearformen zu, und zwar nach folgendem Gesichtspunkte: Ist $k^{(r)}$ ein reeller Körper, so ordnen wir demselben die Linearform

$$f_r = \omega_1^{(r)} u_1 + \cdots + \omega_m^{(r)} u_m$$

zu; ist dagegen $k^{(s)}$ ein imaginärer Körper und $k^{(s')}$ der zu demselben conjugirt imaginäre Körper, so ordnen wir den beiden Körpern $k^{(s)}$ und $k^{(s')}$ die beiden Linearformen

$$(8.) \quad \begin{cases} f_s = \dfrac{1}{\sqrt{2}} \{(\omega_1^{(s)} + \omega_1^{(s')}) u_1 + \cdots + (\omega_m^{(s)} + \omega_m^{(s')}) u_m\}, \\[2ex] f_{s'} = \dfrac{1}{i\sqrt{2}} \{(\omega_1^{(s)} - \omega_1^{(s')}) u_1 + \cdots + (\omega_m^{(s)} - \omega_m^{(s')}) u_m\} \end{cases}$$

zu, deren Coefficienten wiederum reell sind. Die Determinante der m Formen $f_1, \ldots, f_m$ ist, absolut genommen, $= |\sqrt{d}|$. Der Hülfssatz 7 liefert dann unmittelbar die Behauptung, wenn man berücksichtigt, dass für die Paare imaginärer Körper

$$f_s^2 + f_{s'}^2 = 2 |\omega_1^{(s)} u_1 + \cdots + \omega_m^{(s)} u_m|^2$$

ist.

Andererseits folgt leicht die Thatsache:

Satz 43. Wenn der Grad m und eine beliebige positive Constante $\varkappa$ gegeben ist, so existirt nur eine endliche Anzahl von ganzen algebraischen Zahlen $m$ten Grades, die nebst allen ihren Conjugirten, absolut genommen, $< \varkappa$ sind.

Beweis. Die m ganzzahligen Coefficienten der Gleichung, der eine solche ganze Zahl genügt, müssen absolut sämtlich unterhalb einer nur von m und $\varkappa$ abhängigen Grenze liegen; sie sind daher ihrer Anzahl nach beschränkt.

§ 18.

Sätze über die absolute Grösse der Körperdiscriminante.

Wir beweisen die beiden folgenden Sätze:

Satz 44. *Die Discriminante d eines Zahlkörpers k ist stets verschieden von* ± 1 [*Minkowski*[1, 2, 3]].

Satz 45. *Es giebt nur eine endliche Anzahl von Körpern mten Grades mit gegebener Discriminante d.* [*Hermite*[1,2], *Minkowski*[3].]

Zum Beweise dieser Sätze dient der folgende Hülfssatz:

Hülfssatz 8. Wenn $f_1, \ldots, f_m$ die in Formel (8) definirten m reellen Linearformen der Unbestimmten $u_1, \ldots, u_m$ bedeuten, so existirt im Körper k stets eine solche von 0 verschiedene ganze Zahl $\alpha = a_1\omega_1 + \cdots + a_m\omega_m$, für welche die absoluten Beträge dieser Formen für $u_1 = a_1, \ldots, u_m = a_m$ den Bedingungen

$$(9.)\quad |f_1| \leqq |\sqrt{d}|, \quad |f_2| < 1, \quad |f_3| < 1, \quad \ldots, \quad |f_m| < 1$$

genügen.

Beweis. Nach Satz 43 kann es nur eine endliche Anzahl von ganzen Zahlen $\alpha, \alpha_1, \alpha_2, \ldots$ im Körper k geben, welche die Bedingungen

$$|f_1| < |\sqrt{d}| + 1, \quad |f_2| < 1, \quad \ldots, \quad |f_m| < 1$$

erfüllen. Diejenige unter diesen Zahlen $\alpha, \alpha_1, \alpha_2, \ldots$, für welche $|f_1|$ den kleinsten Wert besitzt, sei α, und dieser kleinste Wert selbst werde mit φ bezeichnet. Sollte es keine solche Zahl α geben, so setze man $\varphi = |\sqrt{d}| + 1$. Fällt nun $\varphi \leqq |\sqrt{d}|$ aus, so ist die Richtigkeit des Hülfssatzes 8 offenbar. Im anderen Falle bestimmen wir eine positive Zahl ε derart, dass $(1+\varepsilon)^{m-1}|\sqrt{d}| < \varphi$ wird. Nach Hülfssatz 7 giebt es dann stets ein System ganzer rationaler Zahlen $u_1, \ldots, u_m$ von der Art, dass

$$|f_1| \leqq (1+\varepsilon)^{m-1}|\sqrt{d}|, \quad |f_2| \leqq \frac{1}{1+\varepsilon}, \quad \ldots, \quad |f_m| \leqq \frac{1}{1+\varepsilon}$$

und folglich

$$|f_1| < \varphi, \qquad |f_2| < 1, \qquad \ldots, \quad |f_m| < 1$$

wird; dies steht mit der von uns getroffenen Wahl der Zahl α im Widerspruch.

Um nun die beiden Sätze 44 und 45 zu beweisen, verfahren wir wie folgt. Ist $k = k^{(1)}$ ein reeller Körper, so ist die Form f_1 eine völlig bestimmte. Ist jedoch $k^{(1)}$ ein imaginärer Körper und $k^{(2)}$ der zu ihm conjugirte, so stehen uns für f_1 zwei Formen zur Auswahl; wir setzen

$$f_1 = \frac{1}{i\sqrt{2}}\{(\omega_1^{(1)} - \omega_1^{(2)})u_1 + \cdots + (\omega_m^{(1)} - \omega_m^{(2)})u_m\}.$$

Die Reihenfolge, in der wir die übrigen Formen $f_2, \ldots, f_m$ annehmen, ist gleichgültig. Der Hülfssatz 8 zeigt die Existenz einer ganzen Zahl α, welche den Bedingungen (9) genügt. Andererseits ist

$$\underset{(r)}{\Pi}|f_r|\underset{s,s'}{\Pi}\frac{f_s^2 + f_{s'}^2}{2} = |n(\alpha)|,$$

wo das erste Product über alle Formen f_r, das zweite über alle Formenpaare f_s, $f_{s'}$ zu erstrecken ist. Da notwendig $|n(\alpha)| \geqq 1$ ausfällt, so folgt $|f_1| > 1$ und daher $|\sqrt{d}| > 1$, womit der Satz 44 bewiesen ist.

Zugleich folgt aus den Ungleichungen $|f_1| > 1$, $|f_2| < 1$, $|f_3| < 1, \ldots$ $\ldots, |f_m| < 1$, dass α eine Zahl des Körpers $k = k^{(1)}$ ist, welche sich von allen ihren Conjugirten unterscheidet, d. h. es ist die Differente $\delta(\alpha) \neq 0$. Nach der Bemerkung auf S. 180 oben ist daher α eine den Körper k bestimmende Zahl. Da ferner d eine vorgeschriebene Zahl ist, so giebt es nach Satz 43 nur eine endliche Anzahl von ganzen algebraischen Zahlen $m$ten Grades, welche nebst ihren Conjugirten den Bedingungen (9) genügen, und daraus folgt unmittelbar die Richtigkeit des Satzes 45.

Der Satz 44 spricht die das Wesen der algebraischen Zahl tief berührende Eigenschaft aus, dass die Discriminante eines jeden Zahlkörpers mindestens eine Primzahl enthalten muss.

Wenn wir statt des zu Anfang dieses Abschnitts genannten und dieser ganzen Untersuchung zu Grunde liegenden Hülfssatzes 6 einen ebenfalls von *Minkowski* aufgestellten schärferen Satz benutzen, so führt die nämliche Schlussweise auf die Thatsache, dass der absolute Betrag der Discriminante eines Körpers $m$ten Grades sicherlich immer die Grösse $\left(\frac{\pi}{4}\right)^{2r_2}\left(\frac{m^m}{m!}\right)^2$ und daher umsomehr die Grösse $\left(\frac{\pi}{4}\right)^{2r_2}\frac{e^{2m-\frac{1}{6m}}}{2\pi m}$ übertrifft, wo r_2 die Anzahl derjenigen imaginären Körperpaare bedeutet, welche unter den m conjugirten Körpern $k^{(1)}, \ldots, k^{(m)}$ vorhanden sind [*Minkowski*[1, 2, 3]].

Die letztere Thatsache, in entsprechender Weise verwertet, zeigt, dass auch unter den Körpern aller möglicher Grade nur eine endliche Anzahl vorhanden sein kann, welche die vorgeschriebene Discriminante d besitzt.

Aus den nämlichen Principien folgt noch eine Thatsache, die für das nächste Capitel VII von Wichtigkeit ist [*Minkowski*[1, 3]]:

Satz 46. Ist $\mathfrak{a}$ ein vorgelegtes Ideal des Körpers k, so giebt es stets eine ganze von 0 verschiedene Zahl α des Körpers, welche durch $\mathfrak{a}$ teilbar ist, und deren Norm der Bedingung

$$|n(\alpha)| \leqq n(\mathfrak{a})\sqrt{|d|}$$

genügt.

Beweis. Sind

$$\iota_1 = a_{11}\,\omega_1 + \cdots + a_{1m}\,\omega_m,$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$\iota_m = a_{m1}\,\omega_1 + \cdots + a_{mm}\,\omega_m$$

die m Basiszahlen des Ideals $\mathfrak{a}$, so mögen aus denselben genau, wie dies vorhin mittelst $\omega_1, \ldots, \omega_m$ geschah, m lineare Formen $f_1, \ldots, f_m$ mit reellen Coefficienten gebildet werden; die Determinante dieser m Formen ist dann dem Werte nach gleich

$$\begin{vmatrix} \iota_1^{(1)}, & \ldots, & \iota_m^{(1)} \\ \cdot & \cdot & \cdot \\ \iota_1^{(m)}, & \ldots, & \iota_m^{(m)} \end{vmatrix} = \begin{vmatrix} a_{11}, & \ldots, & a_{1m} \\ \cdot & \cdot & \cdot \\ a_{m1}, & \ldots, & a_{mm} \end{vmatrix} \begin{vmatrix} \omega_1^{(1)}, & \ldots, & \omega_m^{(1)} \\ \cdot & \cdot & \cdot \\ \omega_1^{(m)}, & \ldots, & \omega_m^{(m)} \end{vmatrix}$$

und folglich nach Satz 19, absolut genommen, gleich $|n(\mathfrak{a})\sqrt{d}|$. Ordnen wir nun den Formen $f_1, \ldots, f_m$ je eine von irgend m reellen positiven Constanten $\varkappa_1, \ldots, \varkappa_m$ zu, deren Product $= |n(\mathfrak{a})\sqrt{d}|$ ist, und welche den Bedingungen $\varkappa_s = \varkappa_{s'}$ genügen, falls $k^{(s)}$ und $k^{(s')}$ conjugirt imaginäre Körper sind, so folgt aus Satz 42 die Richtigkeit des Satzes 46.

§ 19.

Der Satz von der Existenz der Einheiten eines Körpers. Ein Hülfssatz über die Existenz einer Einheit von besonderer Eigenschaft.

Die wichtigste Grundlage für das tiefere Studium der ganzen algebraischen Zahlen bildet der folgende fundamentale Satz über die Einheiten des Körpers k [*Dirichlet*[13, 14, 16], *Dedekind*[1], *Kronecker*[18, 20], *Minkowski*[3]].

Eine ganze Zahl ε des Körpers k, deren reciproker Wert $\frac{1}{\varepsilon}$ wiederum eine ganze Zahl ist, heisst eine **Einheit** des Körpers k. Die Norm einer Einheit ist $= \pm 1$; umgekehrt, wenn die Norm einer ganzen Zahl des Körpers $= \pm 1$ wird, so ist diese eine Einheit des Körpers.

Satz 47. Sind unter den m conjugirten Körpern $k^{(1)}, \ldots, k^{(m)}$ r_1 reelle Körper und $r_2 = \frac{m - r_1}{2}$ imaginäre Körperpaare vorhanden, so giebt es im Körper $k = k^{(1)}$ ein System von $r = r_1 + r_2 - 1$ Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ von der Beschaffenheit, dass jede vorhandene Einheit ε des Körpers k auf eine und nur auf eine Weise in der Gestalt

$$\varepsilon = \varrho\,\varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r}$$

dargestellt werden kann, wo $a_1, \ldots, a_r$ ganze rationale Zahlen sind, und wo ϱ eine in k vorkommende Einheitswurzel bedeutet.

Um den Beweis dieses Satzes vorzubereiten, ordnen wir die m conjugirten Körper $k^{(1)}, \ldots, k^{(m)}$ in bestimmter Weise, wie folgt, an. Voran stellen wir die r_1 reellen Körper $k^{(1)}, \ldots, k^{(r_1)}$; dann wählen wir aus

jedem der r_2 Paare conjugirt imaginärer Körper je einen aus; diese Körper seien: $k^{(r_1+1)}, \ldots, k^{(r_1+r_2)}$; darauf lassen wir die zu diesen conjugirt imaginären Körper folgen: $k^{(r_1+r_2+1)}, \ldots, k^{(m)}$. Wir bilden nun mit den m beliebigen reellen Veränderlichen $u_1, \ldots, u_m$ die m Linearformen

$$\xi_s = \omega_1^{(s)} u_1 + \cdots + \omega_m^{(s)} u_m, \quad (s = 1, 2, \ldots, m)$$

und schreiben noch $\xi_1 = \xi$. Sind $\xi_1, \ldots, \xi_m$ sämtlich $\neq 0$, so setzen wir im Falle, dass $k^{(s)}$ ein reeller Körper ist,

$$\log|\xi_s| = l_s(\xi)$$

und im Falle, dass $k^{(s)}$ und $k^{(s')}$ conjugirt imaginäre Körper sind,

$$\log(\xi_s) = \tfrac{1}{2} l_s(\xi) - i l_{s'}(\xi),$$
$$\log(\xi_{s'}) = \tfrac{1}{2} l_s(\xi) + i l_{s'}(\xi),$$

wo $l_1(\xi), \ldots, l_m(\xi)$ sämtlich reelle Grössen sind und insbesondere die Werte $l_{s'}(\xi)$ den Ungleichungen

$$0 \leqq l_{s'}(\xi) < 2\pi$$

genügen sollen; die Grössen $l_1(\xi), \ldots, l_m(\xi)$ sind hierdurch als eindeutige reelle Functionen der reellen Veränderlichen $u_1, \ldots, u_m$ definirt; sie sollen die **Logarithmen zur Form** ξ heissen. Bezeichnet ferner $ln(\xi)$ den reellen Teil des Logarithmus von $n(\xi)$, so ist

$$l_1(\xi) + \cdots + l_{r+1}(\xi) = ln(\xi).$$

Sind $u_1, \ldots, u_m$ ganze rationale Zahlen, die nicht sämtlich verschwinden, so stellt $\xi = \xi_1$ eine ganze von 0 verschiedene Zahl α des Körpers $k = k^{(1)}$ dar. Die Grössen $l_1(\xi), \ldots, l_m(\xi)$ sind dann eindeutig durch die Zahl α bestimmt und sollen die **Logarithmen zur Zahl** α heissen. Ist ε eine Einheit des Körpers k, so besteht wegen $n(\varepsilon) = \pm 1$ die Gleichung

$$l_1(\varepsilon) + l_2(\varepsilon) + \cdots + l_{r+1}(\varepsilon) = 0.$$

Die reellen Variabeln $u_1, \ldots, u_m$ sind umgekehrt durch die Werte der Logarithmen $l_1(\xi), \ldots, l_m(\xi)$ 2^{r_1}-deutig bestimmt, da durch letztere die r_1 reellen Werte $\xi_1, \ldots, \xi_{r_1}$ nur bis auf das Vorzeichen, dagegen die übrigen conjugirt imaginären Wertepaare $\xi_{r_1+1}, \ldots, \xi_m$ vollständig bestimmt sind.

Um die später anzuwendende Functionaldeterminante dieses Abhängigkeitsverhältnisses zu berechnen, bezeichnen wir, wenn $f_1, \ldots, f_m$ m beliebige Functionen der Variabeln $x_1, \ldots, x_m$ sind, die Functional-

determinante der $f_1, \ldots, f_m$ bezüglich der $x_1, \ldots, x_m$ mit $\dfrac{f_1, \ldots, f_m}{x_1, \ldots, x_m}$; dann gelten für die absoluten Beträge die Formeln

$$\left|\frac{u_1, \ldots, u_m}{\xi_1, \ldots, \xi_m}\right| = \frac{1}{|\sqrt{d}|}, \quad \left|\frac{\xi_1, \ldots, \xi_m}{l_1(\xi), \ldots, l_m(\xi)}\right| = |\xi_1 \cdots \xi_m| = |n(\xi)|,$$

woraus durch Multiplication der Wert von $\left|\dfrac{u_1, \ldots, u_m}{l_1(\xi), \ldots, l_m(\xi)}\right|$ sich ergiebt.

Im Folgenden werden vornehmlich die ersten r Logarithmen $l_1, \ldots, l_r$ zur Form ξ oder zu einer Zahl α betrachtet. Für die r ersten Logarithmen zu Formen ξ, η oder Zahlen α, β gelten offenbar die Gleichungen

$$\left.\begin{aligned} l_s(\xi\eta) &= l_s(\xi) + l_s(\eta) \\ l_s(\alpha\beta) &= l_s(\alpha) + l_s(\beta) \end{aligned}\right\} \qquad (s = 1, \ldots, r).$$

Nunmehr beweisen wir folgende Thatsache:

Hülfssatz 9. Im Körper k giebt es stets eine Einheit ε, welche die Bedingung

$$\gamma_1 l_1(\varepsilon) + \cdots + \gamma_r l_r(\varepsilon) \neq 0$$

erfüllt, wobei $\gamma_1, \ldots, \gamma_r$ beliebige vorgeschriebene, nicht sämtlich verschwindende reelle Constante sind.

Beweis. Man setze, wenn ω irgend eine ganze von 0 verschiedene Zahl in k bedeutet, zur Abkürzung

$$L(\omega) = \gamma_1 l_1(\omega) + \cdots + \gamma_r l_r(\omega);$$

ferner bestimme man irgend ein System von r reellen Grössen $\lambda_1, \ldots, \lambda_r$, so dass $\gamma_1 \lambda_1 + \cdots + \gamma_r \lambda_r = 1$ wird, und setze dann

$$A_1 = e^{\lambda_1 t}, \quad \ldots, \quad A_{r_1} = e^{\lambda_{r_1} t}, \quad A_{r_1+1} = e^{\frac{1}{2}\lambda_{r_1+1} t}, \quad \ldots, \quad A_r e^{\frac{1}{2}\lambda_r t},$$

wo t einen willkürlichen reellen Parameter bezeichnet. Es sind dann zwei Fälle zu unterscheiden, je nachdem sämtliche m conjugirte Körper $k^{(1)}, \ldots, k^{(m)}$ reell sind oder nicht. Im ersten Falle ordnen wir den $r = m-1$ Körpern $k^{(1)}, \ldots, k^{(r)}$ die Grössen $A_1, \ldots, A_r$ und dem übrig gebliebenen letzten Körper $k^{(m)}$ die Constante $A_m = \dfrac{|\sqrt{d}|}{A_1 \cdots A_{m-1}}$ zu. Im zweiten Fall ordnen wir den Körpern $k^{(1)}, \ldots, k^{(r)}$ wiederum die Grössen $A_1, \ldots, A_r$ zu, dem imaginären Körper $k^{(r+1)}$ werde die

Constante $\varDelta_{r+1} = \left|\left\{\frac{\sqrt{d}}{\varDelta_1 \cdots \varDelta_{r_1}\, \varDelta_{r_1+1}^2 \cdots \varDelta_r^2}\right\}^{\frac{1}{2}}\right|$ zugeordnet. Endlich ordnen wir den $m-r-1$ übrig gebliebenen imaginären Körpern $k^{(r+2)}, \ldots, k^{(m)}$ bezüglich die nämlichen Constanten zu, wie sie bereits den conjugirt imaginären Körpern zugeordnet sind; wir bezeichnen die betreffenden Constanten mit $\varDelta_{r+2}, \ldots, \varDelta_m$. In beiden Fällen wird das Product

$$\varDelta_1 \cdots \varDelta_m = |\sqrt{d}\,|,$$

und die Constanten $\varDelta_1, \ldots, \varDelta_m$ erfüllen mithin die Bedingungen, denen die Constanten $\varkappa_1, \ldots, \varkappa_m$ des Satzes 42 genügen sollten.

Dem Satz 42 zufolge giebt es daher im Körper k eine von 0 verschiedene Zahl α derart, dass

$$(10.) \qquad |\alpha^{(1)}| \leqq \varDelta_1, \quad \ldots, \quad |\alpha^{(m)}| \leqq \varDelta_m$$

und folglich zugleich $|n(\alpha)| \leqq |\sqrt{d}\,|$ wird. Wegen $|n(\alpha)| \geqq 1$ ist für alle Werte $s = 1, 2, \ldots, m$:

$$|\alpha^{(s)}| \geqq \frac{1}{|\alpha^{(1)}| \cdots |\alpha^{(s-1)}|\, |\alpha^{(s+1)}| \cdots |\alpha^{(m)}|};$$

wenn wir daher die Ungleichungen

$$\left|\frac{1}{\alpha^{(1)}}\right| \geqq \frac{1}{\varDelta_1}, \quad \ldots, \quad \left|\frac{1}{\alpha^{(m)}}\right| \geqq \frac{1}{\varDelta_m},$$

$$\varDelta_1 \cdots \varDelta_m = |\sqrt{d}|$$

berücksichtigen, so folgt

$$(11.) \qquad |\alpha^{(s)}| \geqq \frac{\varDelta_s}{|\sqrt{d}\,|}.$$

Aus den beiden Ungleichungen (10.) und (11.) ergiebt sich, wenn der reelle Wert von $\log|\sqrt{d}\,|$ mit δ bezeichnet wird,

$$\left.\begin{array}{l} \lambda_s t \geqq l_s(\alpha) \geqq \lambda_s t - 2\delta \\ \text{oder} \\ 0 \leqq |l_s(\alpha) - \lambda_s t| \leqq 2\delta \end{array}\right\} \quad (s = 1, 2, \ldots, r),$$

woraus zu ersehen ist, dass der Ausdruck

$$\gamma_1\{l_1(\alpha) - \lambda_1 t\} + \cdots + \gamma_r\{l_1(\alpha) - \lambda_r t\} = L(\alpha) - t$$

zwischen gewissen endlichen Grenzen δ_1 und $\delta_2 > \delta_1$ liegt, welche nur von d und $\gamma_1, \ldots, \gamma_r$, dagegen nicht von dem Wert des Parameters t abhängig sind.

Es werde nun eine Grösse $\varDelta > \delta_2 - \delta_1$ bestimmt; bringt man dann

für t der Reihe nach die Werte $t = 0, \varDelta, 2\varDelta, 3\varDelta, \ldots$ in Anwendung, so wird man durch das beschriebene Verfahren eine unendliche Reihe von Zahlen $\alpha, \beta, \gamma, \ldots$ erhalten, deren Normen, absolut genommen, sämtlich $\leqq |\sqrt{d}|$ sind, und für welche ausserdem die Bedingungen $L(\alpha) < L(\beta) < L(\gamma) < \cdots$ erfüllt sind. Da in den ganzen rationalen Zahlen, deren absolute Beträge $\leqq |\sqrt{d}|$ sind, nur eine endliche Anzahl unter einander verschiedener Ideale als Factoren aufgehen, so kann in der unendlichen Reihe der Hauptideale $(\alpha), (\beta), (\gamma), \ldots$ nur eine endliche Anzahl verschiedener Ideale vorkommen, und es werden daher unendlich viele Male zwei dieser Ideale einander gleich. Ist etwa $(\alpha) = (\beta)$, so stellt $\varepsilon = \frac{\beta}{\alpha}$ eine Einheit dar, welche wegen $L(\varepsilon) = L(\beta) - L(\alpha) > 0$ die Bedingung unseres Hülfssatzes 9 erfüllt.

§ 20.

Beweis des Satzes von der Existenz der Einheiten.

Um nunmehr den Satz 47 zu beweisen, wählen wir dem Hülfssatz 9 gemäss in k eine Einheit η_1, für welche $l_1(\eta_1) \neq 0$ ausfällt, dann eine Einheit η_2, für welche die Determinante

$$\begin{vmatrix} l_1(\eta_1), & l_1(\eta_2) \\ l_2(\eta_1), & l_2(\eta_2) \end{vmatrix} \neq 0,$$

ferner eine Einheit η_3, für welche die Determinante

$$\begin{vmatrix} l_1(\eta_1), & l_1(\eta_2), & l_1(\eta_3) \\ l_2(\eta_1), & l_2(\eta_2), & l_2(\eta_3) \\ l_3(\eta_1), & l_3(\eta_2), & l_3(\eta_3) \end{vmatrix} \neq 0$$

ausfällt u. s. f.; man gelangt so zu einem System von Einheiten $\eta_1, \ldots, \eta_r$, für welche schliesslich die Determinante

$$\begin{vmatrix} l_1(\eta_1), & \ldots, & l_1(\eta_r) \\ \cdot & \cdot & \cdot \\ l_r(\eta_1), & \ldots, & l_r(\eta_r) \end{vmatrix} \neq 0$$

ist. Infolge dessen lassen sich, wenn $\boldsymbol{H}$ eine beliebige Einheit im Körper ist, die r ersten Logarithmen zu $\boldsymbol{H}$ stets in die Gestalt

$$\begin{aligned} l_1(\boldsymbol{H}) &= e_1 l_1(\eta_1) + \cdots + e_r l_1(\eta_r), \\ &\cdots\cdots\cdots \\ l_r(\boldsymbol{H}) &= e_1 l_r(\eta_1) + \cdots + e_r l_r(\eta_r) \end{aligned}$$

bringen, wo $e_1, \ldots, e_r$ reelle Grössen bedeuten. Diese Darstellung wiederum zeigt, dass

$$l_1(H) = m_1 l_1(\eta_1) + \cdots + m_r l_1(\eta_r) + E_1,$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$l_r(H) = m_1 l_r(\eta_1) + \cdots + m_r l_r(\eta_r) + E_r$$

gesetzt werden kann, wo $m_1, \ldots, m_r$ die numerisch grössten ganzen rationalen, bezüglich in $e_1, \ldots, e_r$ enthaltenen Zahlen bedeuten. Die Zahlen $E_1, \ldots, E_r$ sind nun ebenfalls von der Gestalt

$$E_1 = \mu_1 l_1(\eta_1) + \cdots + \mu_r l_1(\eta_r),$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$E_r = \mu_1 l_r(\eta_1) + \cdots + \mu_r l_r(\eta_r).$$

Da hierin $\mu_1, \ldots, \mu_r$ reelle Grössen $\geqq 0$ und < 1 bedeuten, so liegen die Werte $E_1, \ldots, E_r$, absolut genommen, sämtlich unterhalb einer Grenze $\varkappa$, welche nicht von H abhängig ist, d. h. die sämtlichen r ersten Logarithmen zur Einheit

$$\overline{H} = \frac{H}{\eta_1^{m_1} \cdots \eta_r^{m_r}}$$

liegen absolut unterhalb der Grenze $\varkappa$. Wegen $l_1(\overline{H}) + \cdots + l_{r+1}(\overline{H}) = 0$ liegt daher der absolute Wert von $l_{r+1}(\overline{H})$ unterhalb der Grenze $r\varkappa$, und mithin bestehen die Ungleichungen

$$|\overline{H}^{(1)}| < e^{\varkappa}, \quad \ldots, \quad |\overline{H}^{(r)}| < e^{\varkappa}, \quad |\overline{H}^{(r+1)}| < e^{r\varkappa},$$

d. h. sämtliche conjugirten Werte der Einheit $\overline{H}$ sind absolut kleiner als die Grösse $e^{r\varkappa}$.

Nach Satz 43 kann nur eine endliche Anzahl solcher Einheiten existiren. Bezeichnen wir dieselben mit $H_1, \ldots, H_G$, so folgt $\overline{H} = H_S$ oder $H = H_S \eta_1^{m_1} \ldots \eta_r^{m_r}$, wo S einen der Werte $1, 2, \ldots, G$ hat. Ist H_T eine beliebige jener G Einheiten $H_1, \ldots, H_G$, und bildet man die ersten $G+1$ Potenzen von H_T, so werden nach dem eben Bewiesenen irgend zwei von diesen Potenzen sich in der Gestalt $H_S \eta_1^{m'_1} \ldots \eta_r^{m'_r}$ bezüglich $H_S \eta_1^{m''_1} \ldots \eta_r^{m''_r}$ darstellen, wo H_S beidemal die gleiche jener G Einheiten bezeichnet; ihr Quotient besitzt mithin eine Darstellung von der Gestalt $\eta_1^{m_1} \ldots \eta_r^{m_r}$. Hiermit ist bewiesen, dass für jede Einheit H_T ein Exponent M_T existirt derart, dass $H_T^{M_T}$ ein Product von Potenzen

der Einheiten $\eta_1, \ldots, \eta_r$ ist. Bezeichnen wir das kleinste gemeinschaftliche Vielfache aller G Exponenten $M_1, \ldots, M_G$ mit M, so hat dieser Exponent M für alle G Einheiten $H_1, \ldots, H_G$ zugleich jene Eigenschaft, und hieraus folgt, dass die r ersten Logarithmen zu einer jeden beliebigen Einheit H des Körpers k die Darstellung

$$(12.)\quad \begin{cases} l_1(H) = \dfrac{m_1 l_1(\eta_1)+\cdots+m_r l_1(\eta_r)}{M}, \\ \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot \\ l_r(H) = \dfrac{m_1 l_r(\eta_1)+\cdots+m_r l_r(\eta_r)}{M} \end{cases}$$

gestatten, wo $m_1, \ldots, m_r$ ganze rationale Zahlen sind.

Nunmehr wenden wir auf dieses unendliche System (12.) der Logarithmen aller Einheiten die nämliche Schlussweise an, wie sie in Satz 5 (§ 3) zum Beweise der Existenz einer Körperbasis auseinandergesetzt worden ist; dann folgt, dass es ein System von r Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ giebt, durch deren zugehörige Logarithmen die Logarithmen zu jeder beliebigen Einheit H des Körpers sich in der Gestalt

$$\begin{aligned} l_1(H) &= a_1 l_1(\varepsilon_1)+\cdots+a_r l_1(\varepsilon_r), \\ &\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot \\ l_r(H) &= a_1 l_r(\varepsilon_1)+\cdots+a_r l_r(\varepsilon_r) \end{aligned}$$

ausdrücken lassen, wo $a_1, \ldots, a_r$ ganze rationale Zahlen sind. Dieses System von Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ genügt den Bedingungen des Satzes 47.

In der That: ist H eine beliebige Einheit, deren zugehörige Logarithmen obige Gestalt besitzen, so ist $\varrho = \dfrac{H}{\varepsilon_1^{a_1}\ldots\varepsilon_r^{a_r}}$ eine Einheit, deren zugehörige Logarithmen offenbar sämtlich $=0$ sind. Eine solche Einheit ϱ ist notwendig eine Einheitswurzel. Denn nach dem vorhin Bewiesenen ist $\varrho^M = \eta_1^{m_1}\ldots\eta_r^{m_r}$, wo $m_1, \ldots, m_r$ gewisse ganze rationale Zahlen sind. Durch Uebergang zu den Logarithmen folgt daraus

$$\begin{aligned} m_1 l_1(\eta_1)+\cdots+m_r l_1(\eta_r) &= 0, \\ \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot&\quad\cdot\quad\cdot\quad\cdot \\ m_1 l_r(\eta_1)+\cdots+m_r l_r(\eta_r) &= 0, \end{aligned}$$

d. h. $m_1 = 0, \ldots, m_r = 0$ und $\varrho^M = 1$. Hieraus ergiebt sich die Darstellung der Einheit H, welche unser Satz 47 verlangt.

Aus der Bestimmungsweise der Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ folgt leicht:

$$\begin{vmatrix} l_1(\eta_1), & \ldots, & l_1(\eta_r) \\ \cdot & \cdot\;\cdot\;\cdot & \cdot \\ l_r(\eta_1), & \ldots, & l_r(\eta_r) \end{vmatrix} = AR,$$

wo A eine ganze rationale Zahl bedeutet und zur Abkürzung

$$R = \begin{vmatrix} l_1(\varepsilon_1), & \ldots, & l_1(\varepsilon_r) \\ \cdot & \cdot\;\cdot\;\cdot & \cdot \\ l_r(\varepsilon_1), & \ldots, & l_r(\varepsilon_r) \end{vmatrix}$$

gesetzt ist. Diese Determinante R ist $\neq 0$, und hieraus folgt, dass die Darstellung der Einheit H durch die Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ nur auf eine Weise geschehen kann. Der Beweis des fundamentalen Satzes 47 ist somit in allen Teilen erbracht.

§ 21.

Die Grundeinheiten. Der Regulator des Körpers. Ein System von unabhängigen Einheiten.

Das System der Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ mit der in Satz 47 dargelegten Eigenschaft heisst ein **System von Grundeinheiten** des Körpers k. Es folgt leicht, dass wenn $\varepsilon_1^*, \ldots, \varepsilon_r^*$ ein anderes System von Grundeinheiten bedeutet, die Determinante aus den zugehörigen r Systemen von je r ersten Logarithmen bis auf das Vorzeichen mit R übereinstimmt. Wir wählen die Reihenfolge der Grundeinheiten stets so, dass R eine positive Zahl wird. Die Zahl R ist dann durch den Körper k eindeutig bestimmt und wird der **Regulator des Körpers** k genannt.

Beim obigen Beweise des Hauptsatzes 47 erkannten wir zugleich, dass eine Einheit, deren zugehörige Logarithmen sämtlich $= 0$ sind, notwendig eine Einheitswurzel ist. Diese Thatsache erhält in dem folgenden Satz Ausdruck, welcher sich übrigens auch in unmittelbarer Weise leicht begründen lässt [*Kronecker* [6], *Minkowski* [3]]:

Satz 48. Eine jede Einheit, die selbst und deren Conjugirte sämtlich den absoluten Betrag 1 besitzen, ist eine Einheitswurzel.

Da in jedem Zahlkörper die beiden Einheitswurzeln $+1$ und -1 vorkommen, so ist die Anzahl aller Einheitswurzeln in k stets gerade; sie kann offenbar nur dann > 2 sein, wenn alle m conjugirten Körper imaginär sind.

Ein beliebiges System von t Einheiten $\eta_1, \ldots, \eta_t$ heisst ein **System von t unabhängigen Einheiten,** wenn zwischen denselben keine Gleichung von der Gestalt $\eta_1^{m_1} \ldots \eta_t^{m_t} = 1$ besteht, wo $m_1, \ldots, m_t$ ganze rationale, nicht sämtlich verschwindende Zahlen sind. Die Zahl t ist stets $\leqq r$; insbesondere bilden die Grundeinheiten $\varepsilon_1, \ldots, \varepsilon_r$ ein System von r unabhängigen Einheiten. Hat man andererseits irgend ein System von r unabhängigen Einheiten $\eta_1, \ldots, \eta_r$, so existirt stets eine ganze rationale Zahl M von der Art, dass für jede beliebige Einheit ε des Körpers k eine Gleichung von der Gestalt $\varepsilon^M = \eta_1^{m_1} \ldots \eta_r^{m_r}$ gilt, wo die Exponenten $m_1, \ldots, m_r$ ganze rationale Zahlen sind. Ist nämlich $\eta_s = \varrho_s \varepsilon_1^{a_{1s}} \ldots \varepsilon_r^{a_{rs}}$ für $s = 1, 2, \ldots, r$, wo ϱ_s Einheitswurzeln und $a_{1s}, \ldots, a_{rs}$ ganzzahlige Exponenten sind, so ist die Determinante der ganzzahligen Exponenten $a_{11}, \ldots, a_{rr}$ wegen der vorausgesetzten Unabhängigkeit der Einheiten $\eta_1, \ldots, \eta_r$ notwendig $\neq 0$. Wird diese Determinante A genannt, so folgt, dass die Ate Potenz jeder beliebigen Einheit ε des Körpers gleich einem Product von Potenzen der Einheiten $\eta_1, \ldots, \eta_r$, multiplicirt in eine Einheitswurzel ϱ, wird. Ist $\varrho^E = 1$ für alle Einheitswurzeln ϱ in k, so ist offenbar die ganze Zahl $M = AE$ von der gewünschten Beschaffenheit.

Der obige Beweis unseres Hauptsatzes 47 zeigt zugleich die Möglichkeit, die Grundeinheiten $\varepsilon_1, \ldots, \varepsilon_r$ durch eine endliche Anzahl von rationalen Operationen aufzustellen. Die eingehendere Behandlung der Frage nach der einfachsten Berechnung der Einheiten führt auf die Theorie der kettenbruchähnlichen Algorithmen, wobei dann die weitere Frage nach der Periodicität solcher Entwickelungen im Vordergrund des Interesses steht [*Minkowski*[3, 4]].

Capitel VII.

Die Idealklassen des Körpers.

§ 22.

Die Idealklasse. Die Endlichkeit der Anzahl der Idealklassen.

Jede ganze Zahl des Zahlkörpers k bestimmt ein Hauptideal; jede **gebrochene,** d. h. nicht ganze Zahl $\varkappa$ in k ist der Quotient zweier ganzen Zahlen α und β und somit als Quotient zweier Ideale $\mathfrak{a}$ und $\mathfrak{b}$ darstellbar: $\varkappa = \dfrac{\alpha}{\beta} = \dfrac{\mathfrak{a}}{\mathfrak{b}}$.

Denken wir die Ideale $\mathfrak{a}$ und $\mathfrak{b}$ von allen gemeinsamen Idealfactoren befreit, so ist diese Darstellung der gebrochenen Zahl $\varkappa$ als Idealquotient eine eindeutig bestimmte. Ist umgekehrt der Quotient $\frac{\mathfrak{a}}{\mathfrak{b}}$ zweier Ideale $\mathfrak{a}$ und $\mathfrak{b}$ — mögen dieselben einen gemeinsamen Teiler haben oder nicht — gleich einer ganzen oder gebrochenen Zahl $\varkappa = \frac{\alpha}{\beta}$ des Körpers, so werden die beiden Ideale $\mathfrak{a}$ und $\mathfrak{b}$ einander **äquivalent** genannt, d. i. in Zeichen $\mathfrak{a} \sim \mathfrak{b}$. Aus $\frac{\alpha}{\beta} = \frac{\mathfrak{a}}{\mathfrak{b}}$ folgt $(\beta)\mathfrak{a} = (\alpha)\mathfrak{b}$, und somit erkennen wir, dass zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ dann und nur dann einander äquivalent sind, wenn sie durch Multiplication mit gewissen Hauptidealen in ein und das nämliche Ideal übergehen. Die Gesamtheit aller Ideale, welche einem gegebenen Ideal äquivalent sind, heisst eine **Idealklasse**. Alle Hauptideale sind dem Ideal (1) äquivalent. Die durch sie gebildete Klasse heisst die **Hauptklasse** und wird mit 1 bezeichnet. Wenn $\mathfrak{a} \sim \mathfrak{a}'$ und $\mathfrak{b} \sim \mathfrak{b}'$ ist, so ist $\mathfrak{a}\mathfrak{a}' \sim \mathfrak{b}\mathfrak{b}'$. Ist A eine das Ideal $\mathfrak{a}$ enthaltende Idealklasse und B eine das Ideal $\mathfrak{b}$ enthaltende Klasse, so wird die Idealklasse, welche das Ideal $\mathfrak{a}\mathfrak{b}$ enthält, das **Product der Idealklassen** A und B genannt und mit AB bezeichnet. Es ist offenbar $1B = B$, und umgekehrt folgt aus $AB = B$ notwendig $A = 1$.

Es ist bisweilen vorteilhaft, auch Idealquotienten in die Rechnung einzuführen: eine Gleichung von der Gestalt $\frac{\mathfrak{a}}{\mathfrak{a}'} = \frac{\mathfrak{b}}{\mathfrak{b}'}$ oder eine Aequivalenz von der Gestalt $\frac{\mathfrak{a}}{\mathfrak{a}'} \sim \frac{\mathfrak{b}}{\mathfrak{b}'}$ soll gleichbedeutend sein mit derjenigen Gleichung oder Aequivalenz zwischen Idealen, welche daraus durch Multiplication mit den in den Nennern stehenden Idealen hervorgeht, d. h. mit der Gleichung $\mathfrak{a}\mathfrak{b}' = \mathfrak{a}'\mathfrak{b}$ bez. mit der Aequivalenz $\mathfrak{a}\mathfrak{b}' \sim \mathfrak{a}'\mathfrak{b}$.

Es gilt der Satz:

Satz 49. Es giebt stets eine und nur eine Idealklasse B, die, mit einer gegebenen Idealklasse A multiplicirt, die Hauptklasse ergiebt.

Beweis. Ist $\mathfrak{a}$ ein Ideal der Klasse A und α eine durch $\mathfrak{a}$ teilbare ganze Zahl, so dass $\alpha = \mathfrak{a}\mathfrak{b}$ gesetzt werden kann, so ist, wenn B die Klasse des Ideals $\mathfrak{b}$ bezeichnet, $AB = 1$. Gäbe es nun noch eine andere Klasse B' so, dass $AB' = 1$ ist, so folgt durch Multiplication mit B die Gleichung $ABB' = B' = B$.

Die Klasse B heisst die zu A **reciproke Klasse** und wird mit A^{-1} bezeichnet.

Es gilt ferner die folgende fundamentale Thatsache:

Satz 50. In jeder Idealklasse giebt es ein Ideal, dessen Norm die absolut genommene Quadratwurzel aus der Körperdiscriminante nicht übersteigt [*Minkowski*[1, 3]]. Die Anzahl der Idealklassen eines Zahlkörpers ist endlich. [*Dedekind*[1], *Kronecker*[16].]

Beweis. Ist A eine beliebige Idealklasse und $\mathfrak{j}$ ein Ideal der reciproken Klasse A^{-1}, so giebt es nach Satz 46 eine ganze, durch $\mathfrak{j}$ teilbare Zahl ι, deren Norm der Bedingung $|n(\iota)| \leqq n(\mathfrak{j})|\sqrt{d}|$ genügt. Setzen wir $\iota = \mathfrak{j}\mathfrak{a}$, so gehört $\mathfrak{a}$ der Idealklasse A an, und wegen $|n(\iota)| = n(\mathfrak{j})n(\mathfrak{a})$ ist $n(\mathfrak{a}) \leqq |\sqrt{d}|$. Es giebt also in der Klasse A ein der letzteren Bedingung genügendes Ideal $\mathfrak{a}$; da aber in den ganzen rationalen Zahlen, welche $\leqq |\sqrt{d}|$ sind, nur eine endliche Anzahl unter einander verschiedener Ideale als Factoren enthalten ist, so folgt auch die Richtigkeit des zweiten Teiles des Satzes 50.

§ 23.

Anwendungen des Satzes von der Endlichkeit der Klassenanzahl.

Der eben bewiesene Satz 50 gestattet mannigfache Folgerungen und Anwendungen, von denen die nachstehenden hervorzuheben sind:

Satz 51. Ist h die Anzahl der Idealklassen, so liefert die $h$te Potenz einer jeden Klasse stets die Hauptklasse.

Beweis. In der Reihe $A, A^2, \ldots, A^{h+1}$ stimmen notwendig zwei Klassen, etwa A^r und A^{r+e}, mit einander überein. Aus $A^r A^e = A^r$ folgt $A^e = 1$. Ist e zugleich der kleinste Exponent (> 0) von der Beschaffenheit, dass $A^e = 1$ wird, so folgt, dass die e Klassen $A^0 = 1$, $A, \ldots, A^{e-1}$ sämtlich unter einander verschieden sind. Ist B eine von diesen e Klassen verschiedene Klasse, so sind die e Klassen $B, AB, \ldots \ldots, A^{e-1}B$ wiederum sämtlich unter einander und von den e vorigen Klassen verschieden; die Fortsetzung dieses Verfahrens zeigt, dass h ein Vielfaches von e sein muss, und hieraus folgt der zu beweisende Satz 51.

Die $h$te Potenz eines jeden beliebigen Ideals $\mathfrak{a}$ ist nach diesem Satz stets ein Hauptideal.

Satz 52. Wenn α und β zwei beliebige ganze Zahlen sind, so giebt es stets eine sowohl in α wie in β aufgehende ganze von 0 verschiedene Zahl γ, welche eine Darstellung $\gamma = \xi\alpha + \eta\beta$ gestattet, wo ξ, η geeignet gewählte ganze Zahlen sind. Die Zahlen γ, ξ, η gehören im allgemeinen nicht dem durch α und β bestimmten Zahlkörper an [*Dedekind*[1]].

Satz 53. Es seien $\varkappa$, ϱ und $\varkappa^*$, ϱ^* zwei Zahlenpaare des Körpers k; damit $\mathfrak{j} = (\varkappa, \varrho) = (\varkappa^*, \varrho^*)$ werde, ist es notwendig und hinreichend, dass man im Körper k vier ganze Zahlen α, β, γ, δ finden kann, deren Determinante $\alpha\delta - \beta\gamma = 1$ ist, und durch welche die Gleichungen

$$\varkappa^* = \alpha\varkappa + \beta\varrho,$$
$$\varrho^* = \gamma\varkappa + \delta\varrho$$

erfüllt sind. [*Hurwitz* [4]].

Beweis. Dass die genannte Bedingung hinreichend ist, folgt aus dem Umstande, dass diese beiden Gleichungen eine Umkehrung von der Gestalt

$$\varkappa = \alpha^*\varkappa^* + \beta^*\varrho^*,$$
$$\varrho = \gamma^*\varkappa^* + \delta^*\varrho^*$$

gestatten, wo α^*, β^*, γ^*, δ^* ganze Zahlen sind. Die Bedingung ist ferner auch notwendig. Bezeichnet nämlich h die Anzahl der Idealklassen, so wird $\mathfrak{j}^h = (\varkappa^h, \varrho^h) = (\varkappa^{*h}, \varrho^{*h}) = (\tau)$, wo τ eine ganze Zahl des Körpers k ist. Es sei

$$\tau = \mu\varkappa^h + \nu\varrho^h = \mu^*\varkappa^{*h} + \nu^*\varrho^{*h},$$

wo μ, ν, μ^*, ν^* ganze Zahlen in k sind; dann erfüllen offenbar die vier ganzen Zahlen

$$\alpha = \frac{\mu\varkappa^*\varkappa^{h-1} + \nu^*\varrho\varrho^{*h-1}}{\tau}, \quad \beta = \frac{\nu\varkappa^*\varrho^{h-1} - \nu^*\varkappa\varrho^{*h-1}}{\tau},$$

$$\gamma = \frac{\mu\varrho^*\varkappa^{h-1} - \mu^*\varrho\varkappa^{*h-1}}{\tau}, \quad \delta = \frac{\nu\varrho^*\varrho^{h-1} + \mu^*\varkappa\varkappa^{*h-1}}{\tau}$$

die Bedingung des Satzes 53. Dass $\alpha\delta - \beta\gamma = 1$ ist, ergiebt sich, wenn man die beiden Determinanten

$$-\tau = \begin{vmatrix} \mu\varkappa^{h-1}, & \varrho \\ \nu\varrho^{h-1}, & -\varkappa \end{vmatrix} \quad \text{und} \quad -\tau = \begin{vmatrix} \varkappa^*, & \nu^*\varrho^{*h-1} \\ \varrho^*, & -\mu^*\varkappa^{*h-1} \end{vmatrix}$$

nach dem Multiplicationssatze mit einander zusammensetzt.

Nach Satz 12 kann ein jedes Ideal in der Gestalt $\mathfrak{j} = (\varkappa, \varrho)$ dargestellt werden. Setzen wir $\vartheta = \frac{\varkappa}{\varrho}$, so bestimmt die ganze oder gebrochene Zahl ϑ vollständig die Idealklasse, zu welcher $\mathfrak{j}$ gehört. Wir nennen ϑ einen dieser Idealklasse zugeordneten **Zahlbruch.** Der Satz 53 zeigt, dass, wenn $\vartheta^* = \frac{\varkappa^*}{\varrho^*}$ ein anderer der Idealklasse zugeordneter Zahlbruch ist, notwendig vier ganze Zahlen α, β, γ, δ mit der Determinante 1 im Körper k existiren müssen derart, dass $\vartheta^* = \frac{\alpha\vartheta + \beta}{\gamma\vartheta + \delta}$ wird.

§ 24.

Aufstellung des Systems der Idealklassen. Engere Fassung des Klassenbegriffes.

Der Beweis des Satzes 50 giebt uns zugleich ein einfaches Mittel an die Hand, durch eine endliche Anzahl rationaler Processe ein volles System von nicht äquivalenten Idealen für jeden gegebenen Körper wirklich aufzustellen. Man braucht nur alle diejenigen Ideale in Betracht zu ziehen, deren Normen $\leqq |\sqrt{d}|$ sind. Um die zwischen diesen Idealen irgend vorhandenen Aequivalenzen sämtlich zu ermitteln, haben wir nur nötig, jedes von ihnen mit jedem zu multipliciren und dann, wenn $\mathfrak{j}$ ein solches Product bedeutet, jedesmal in $\mathfrak{j}$ eine Zahl $\iota \neq 0$ mit absolut kleinster Norm aufzusuchen, um zu sehen, ob $\mathfrak{j} = (\iota)$ ist und somit die Factoren reciproken Klassen angehören. Dass dies ebenfalls nur eine endliche Anzahl von Operationen erfordert, erkennen wir aus dem Satze 46. Ist nämlich $\iota_1, \ldots, \iota_m$ die Basis des Ideals $\mathfrak{j}$, so haben wir nur nötig, $u_1, \ldots, u_m$ als ganze rationale, nicht sämtlich verschwindende Zahlen so zu bestimmen, dass die absoluten Werte der reellen und imaginären Teile von $u_1 \iota_1^{(s)} + \cdots + u_m \iota_m^{(s)}$ für $s = 1, \ldots, m$ sämtlich unter gewissen gegebenen Grenzen bleiben. Hierzu bedarf es nur einer endlichen Anzahl von Versuchen. Auf gleiche Weise sehen wir auch ein, dass für jedes vorgelegte Ideal die Klasse, der dasselbe angehört, stets durch eine endliche Anzahl von rationalen Operationen bestimmt werden kann.

Es werde bemerkt, dass unter Umständen auch eine **engere Fassung des Aequivalenz- und Klassenbegriffes** von Nutzen ist, indem zwei Ideale nur dann äquivalent heissen, wenn ihr Quotient eine ganze oder gebrochene Zahl mit positiver Norm ist [*Dedekind*[1]].

§ 25.

Ein Hülfssatz über den asymptotischen Wert der Anzahl aller Hauptideale, welche durch ein festes Ideal teilbar sind.

Nach dem Vorbilde von *Dirichlet*, welcher die Anzahl der Klassen von binären quadratischen Formen mit gegebener Determinante auf transcendentem Wege ausgedrückt hat [*Dirichlet*[7, 8]], und auf Grund der in Capitel VI erhaltenen Resultate über die Einheiten eines Zahlkörpers gelang es *Dedekind*, eine fundamentale Formel abzuleiten, vermöge welcher sich die Anzahl h der Idealklassen eines beliebigen Zahlkörpers als Grenz-

wert einer gewissen unendlichen Reihe darstellt [*Dedekind*[1]]. Um zu dieser Formel zu gelangen, beweisen wir zunächst folgenden Hülfssatz:

Hülfssatz 10. Ist t eine reelle positive Veränderliche und T die Anzahl aller derjenigen durch das gegebene Ideal $\mathfrak{a}$ teilbaren Hauptideale, deren Normen $\leqq t$ sind, so ist

$$\underset{t=\infty}{L}\frac{T}{t}=\frac{2^{r_1+r_2}\pi^{r_2}}{w}\cdot\frac{1}{n(\mathfrak{a})}\frac{R}{|\sqrt{d}|},$$

wo w die Anzahl der in k vorkommenden Einheitswurzeln und R den Regulator des Körpers k bezeichnet. Die Bedeutung von r_1, r_2 ist in Satz 47 erklärt. L dient zur Abkürzung für Limes.

Beweis. Es sei $\alpha_1, \ldots, \alpha_m$ eine Basis des Ideals $\mathfrak{a}$; jede durch $\mathfrak{a}$ teilbare ganze Zahl besitzt dann die Gestalt:

$$\eta=\eta(v)=v_1\alpha_1+\cdots+v_m\alpha_m=f_1(v)\omega_1+\cdots+f_m(v)\omega_m,$$

wo $v_1, \ldots, v_m$ ganze rationale Zahlen annehmen und $f_1(v), \ldots, f_m(v)$ lineare ganzzahlige Functionen der $v_1, \ldots, v_m$ sind. Wenn wir $v_1, \ldots, v_m$ als reelle Veränderliche ansehen und

$$u_1=\frac{f_1(v)}{\left|\sqrt[m]{n(\eta)}\right|},\quad \ldots,\quad u_m=\frac{f_m(v)}{\left|\sqrt[m]{n(\eta)}\right|},$$

$$\xi=\xi(v)=u_1\omega_1+\cdots+u_m\omega_m=\frac{\eta(v)}{\left|\sqrt[m]{n(\eta)}\right|}$$

setzen, so sind $u_1, \ldots, u_m$ eindeutige Functionen von $v_1, \ldots, v_m$, und ξ ist eine Form, für welche $n(\xi)=\pm 1$ wird. Wir berechnen nun die r ersten Logarithmen zur Form ξ und hieraus r reelle Grössen $e_1(\xi), \ldots, e_r(\xi)$ derart, dass, wenn $\varepsilon_1, \ldots, \varepsilon_r$ ein System von Grundeinheiten bezeichnen,

$$\begin{aligned}
l_1(\xi) &= e_1(\xi)l_1(\varepsilon_1)+\cdots+e_r(\xi)l_1(\varepsilon_r),\\
&\cdots\cdots\cdots\cdots\\
l_r(\xi) &= e_1(\xi)l_r(\varepsilon_1)+\cdots+e_r(\xi)l_r(\varepsilon_r)
\end{aligned}$$

ist; diese r Grössen $e_1, \ldots, e_r$ werden in diesem § 25 kurz die r Exponenten von η genannt.

Nimmt man für $v_1, \ldots, v_m$ ganze rationale, nicht sämtlich verschwindende Zahlen, so ist klar, dass die so entstehende ganze Zahl η stets durch Multiplication mit ganzen Potenzen der Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ in eine solche Zahl verwandelt werden kann, deren Exponenten $e_1, \ldots, e_r$ den Bedingungen

(13) $\qquad 0\leqq e_1<1, \quad \ldots, \quad 0\leqq e_r<1$

genügen. Umgekehrt sehen wir, dass zwei ganze Zahlen η, η^*, deren Exponenten gleich sind, sich nur um einen Factor unterscheiden können, welcher eine Einheitswurzel ist. Wenn daher w die Anzahl der in k liegenden Einheitswurzeln bezeichnet, so ist das w-fache der Anzahl T aller durch $\mathfrak{a}$ teilbaren Hauptideale mit einer Norm $\leqq t$ notwendig gleich der Anzahl der verschiedenen Systeme von ganzzahligen Wertsystemen $v_1, \ldots, v_m$, für welche $|n(\eta)| \leqq t$ ausfällt, und für welche überdies die Exponenten $e_1, \ldots, e_r$ den Bedingungen (13) genügen.

Nunmehr setzen wir

$$\tau = t^{-\frac{1}{m}}, \quad v_1 = \frac{\varphi_1}{\tau}, \quad \ldots, \quad v_m = \frac{\varphi_m}{\tau};$$

dabei bleiben die Form ξ und folglich auch die Grössen $l_1(\xi), \ldots, l_r(\xi)$, $e_1, \ldots, e_r$ von τ unabhängig und enthalten lediglich die m neuen Veränderlichen $\varphi_1, \ldots, \varphi_m$. Die Ungleichung $|n(\eta)| \leqq t$ geht in $|n(\eta(\varphi))| \leqq 1$ über; da ferner in Folge der Bedingungen (13) die r Logarithmen $l_1(\xi), \ldots, l_r(\xi)$ und folglich wegen $l_1(\xi) + \cdots + l_{r+1}(\xi) = ln(\xi) = 0$ auch der Logarithmus $l_{r+1}(\xi)$ absolut unter einer endlichen, durch $\varepsilon_1, \ldots, \varepsilon_r$ bestimmten Grenze liegen, so folgt das Gleiche für die sämtlichen Grössen $|\xi^{(1)}(\varphi)|, \ldots, |\xi^{(m)}(\varphi)|$, und damit liegen wegen $|n(\eta(\varphi))| \leqq 1$ auch die m Grössen $|\eta^{(1)}(\varphi)|, \ldots, |\eta^{(m)}(\varphi)|$ sämtlich unterhalb einer endlichen Grenze. Hieraus folgt, dass die Ungleichungen (13) unter Zuhülfenahme der Ungleichung $|n(\eta(\varphi))| \leqq 1$ in dem durch die m Coordinaten $\varphi_1, \ldots, \varphi_m$ bestimmten m-dimensionalen Raume ein endliches Raumgebiet abgrenzen.

Bedenken wir nun, dass nach den Ausführungen in § 19 S. 215 die Functionswerte $l_1(\eta), \ldots, l_m(\eta)$ die Werte der Variabeln $\varphi_1, \ldots, \varphi_m$ 2^{r_1}-deutig bestimmen, so ist nach der Definition des Begriffs eines vielfachen Integrals

$$\underset{\tau=0}{L}\{wT\tau^m\} = 2^{r_1}\iint\cdots\int d\varphi_1\, d\varphi_2 \ldots d\varphi_m,$$

wo das Integral rechter Hand über das durch die Ungleichungen

$$0 \leqq e_1 \leqq 1, \quad \ldots, \quad 0 \leqq e_r \leqq 1, \quad |n(\eta(\varphi))| \leqq 1$$

bestimmte m-dimensionale Raumgebiet zu erstrecken ist und daher einen endlichen bestimmten Wert besitzt.

Um diesen Wert zu ermitteln, führen wir statt der Integrationsveränderlichen $\varphi_1, \ldots, \varphi_m$ die neuen Veränderlichen

$$\psi_1 = e_1(\xi), \ \ldots, \ \psi_r = e_r(\xi), \ \psi_{r+1} = |n(\eta)|, \ \psi_{r+2} = l_{r+2}(\xi), \ \ldots \\ \ldots, \ \psi_m = l_m(\xi)$$

ein, wo ξ und η von $\varphi_1, \ldots, \varphi_m$ abhängig zu nehmen sind. Da diese m Grössen sämtlich analytische und in dem Integrationsgebiet

$$0 \leqq \psi_1 \leqq 1, \quad \ldots, \quad 0 \leqq \psi_r \leqq 1, \quad 0 \leqq \psi_{r+1} \leqq 1,$$
$$0 \leqq \psi_{r+2} \leqq 2\pi, \quad \ldots, \quad 0 \leqq \psi_m \leqq 2\pi$$

sich regulär verhaltende, eindeutige Functionen von $\varphi_1, \ldots, \varphi_m$ sind, so ist

$$\int \cdots \int d\varphi_1 \cdots d\varphi_m = \int \cdots \int \left| \frac{\varphi_1, \cdots, \varphi_m}{\psi_1, \cdots, \psi_m} \right| d\psi_1 \ldots d\psi_m.$$

Nach den Ausführungen in § 19 S. 216 ist

$$\left| \frac{f_1, \ldots, f_m}{l_1(\eta), \ldots, l_m(\eta)} \right| = \left| \frac{n(\eta)}{\sqrt{d}} \right|.$$

Ferner bestehen wegen

$$ln(\eta) = l_1(\eta) + \cdots + l_{r+1}(\eta), \quad l_s(\xi) = l_s(\eta) - \frac{1}{m} ln(\eta)$$
$$(s = 1, 2, \ldots, r)$$

offenbar die Beziehungen:

$$\left| \frac{l_1(\eta), \ldots, l_r(\eta) \, l_{r+1}(\eta)}{l_1(\eta), \ldots, l_r(\eta), \, ln(\eta)} \right| = 1, \quad \left| \frac{l_1(\eta), \ldots, l_r(\eta), \, ln(\eta)}{l_1(\xi), \ldots, l_r(\xi), \, ln(\eta)} \right| = 1;$$

und da endlich

$$l_{r+2}(\eta) = l_{r+2}(\xi), \quad \ldots, \quad l_m(\eta) = l_m(\xi),$$

$$\left| \frac{ln(\eta)}{n(\eta)} \right| = \frac{1}{|n(\eta)|}, \quad \left| \frac{\varphi_1, \cdots, \varphi_m}{f_1(\varphi), \cdots, f_m(\varphi)} \right| = \frac{1}{n(\mathfrak{a})}, \quad \left| \frac{l_1(\xi), \ldots, l_r(\xi)}{\psi_1, \ldots, \psi_r} \right| = R$$

ist, so ergiebt sich durch Multiplication sämtlicher Gleichungen

$$\left| \frac{\varphi_1, \ldots, \varphi_m}{\psi_1, \ldots, \psi_m} \right| = \frac{R}{n(\mathfrak{a}) |\sqrt{d}|}.$$

Das obige Integral besitzt daher den Wert $\dfrac{(2\pi)^{r_2} R}{n(\mathfrak{a}) |\sqrt{d}|}$; hiermit ist der Beweis für den Hülfssatz 10 erbracht.

Wir setzen im Folgenden zur Abkürzung

$$\varkappa = \frac{2^{r_1 + r_2} \pi^{r_2}}{w} \cdot \frac{R}{|\sqrt{d}|},$$

so dass $\varkappa$ eine durch den Körper allein bestimmte und für diesen charakteristische Grösse bedeutet.

§ 26.
Die Bestimmung der Klassenanzahl durch das Residuum der Function $\zeta(s)$ für $s=1$.

Satz 54. Wenn T die Anzahl aller Ideale einer Klasse A bedeutet, deren Normen $\leqq t$ ausfallen, so ist

$$\underset{t=\infty}{L} \frac{T}{t} = \varkappa.$$

Beweis. Ist $\mathfrak{a}$ ein Ideal der zu A reciproken Klasse A^{-1}, und durchläuft $\mathfrak{x}$ alle Ideale der Klasse A, so stellt das Product $\mathfrak{x}\mathfrak{a}$ alle durch $\mathfrak{a}$ teilbaren Hauptideale und jedes nur einmal dar. Setzen wir daher in der Formel des Hülfssatzes 10. $t=n(\mathfrak{a})t'$, so bedeutet T zugleich die Anzahl der Ideale $\mathfrak{x}$ in A, für welche $n(\mathfrak{x}) < t'$ ist. Nach Fortheben des Factors $n(\mathfrak{a})$ folgt die zu beweisende Formel für $t=t'$.

Da die Zahl $\varkappa$ von der Wahl der Klasse A unabhängig ist, so ergiebt sich unmittelbar aus Satz 54 die folgende Thatsache:

Satz 55. Ist T die Anzahl aller Ideale des Körpers k, deren Normen $\leqq t$ ausfallen, und bedeutet h die Anzahl der Idealklassen, so ist

$$\underset{t=\infty}{L} \frac{T}{t} = h\varkappa.$$

Aus dieser Formel kann mit Hülfe analytischer Methoden ein fundamentaler Ausdruck für die Klassenanzahl h abgeleitet werden. Es ergiebt sich nämlich folgende Thatsache:

Satz 56. *Die unendliche Reihe*

$$\zeta(s) = \sum_{(\mathfrak{j})} \frac{1}{n(\mathfrak{j})^s},$$

in welcher $\mathfrak{j}$ *alle Ideale des Körpers durchläuft, convergirt für reelle Werte von* $s>1$, *und es ist*

$$\underset{s=1}{L} \{(s-1)\zeta(s)\} = h\varkappa.$$

[*Dedekind* [1]].

Beweis. Bezeichnen wir mit $F(n)$ die Anzahl der verschiedenen Ideale mit der Norm n, so ist offenbar, wenn T die in Satz 55 angegebene Bedeutung hat,

$$\underset{t=\infty}{L} \frac{T}{t} = \underset{n=\infty}{L} \frac{F(1)+F(2)+\cdots+F(n)}{n}.$$

Der Limes rechter Hand kann nun, wie folgt, als Grenzwert einer un-

endlichen Reihe dargestellt werden. [*Dirichlet* [15].] Wir ordnen die sämtlichen Ideale $\mathfrak{j}$ des Körpers nach der Grösse ihrer Normen, schreiben die entstehende Reihe $\mathfrak{j}_1, \mathfrak{j}_2, \ldots, \mathfrak{j}_t, \ldots$ und bezeichnen allgemein die Norm von $\mathfrak{j}_t$ mit n_t, dann ist

$$F(1)+\cdots+F(n_t-1) < t \leqq F(1)+\cdots+F(n_t)$$

oder

$$\frac{F(1)+\cdots+F(n_t-1)}{n_t-1}\left(1-\frac{1}{n_t}\right) < \frac{t}{n_t} \leqq \frac{F(1)+\cdots+F(n_t)}{n_t},$$

und hieraus folgt nach Satz 55: $\underset{t=\infty}{L}\frac{t}{n_t}=h\varkappa$, d. h.: wie klein auch die positive Grösse δ gegeben sein mag, es ist stets möglich, die ganze Zahl t so gross zu wählen, dass die Ungleichungen

$$(14)\qquad \frac{h\varkappa-\delta}{t'} < \frac{1}{n_{t'}} < \frac{h\varkappa+\delta}{t'}$$

für alle ganzen Zahlen $t' \geqq t$ gültig sind.

Andererseits ist bekannt, dass, wenn s eine reelle Zahl >1 bedeutet, die Reihe $\sum\limits_{(t)}\frac{1}{t^s}=\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\cdots$ convergirt, und dass $\underset{s=1}{L}\left\{(s-1)\sum\limits_{(t)}\frac{1}{t^s}\right\}=1$ ist. Die letztere Gleichung zeigt, dass auch $\underset{s=1}{L}\left\{(s-1)\sum\limits_{t'}\frac{1}{t'^s}\right\}=1$ ist, wo t' nur alle diejenigen ganzen Zahlen durchlaufen soll, welche oberhalb einer beliebig hohen Grenze t gelegen sind. Zunächst folgt aus der Convergenz der Reihe $\sum\frac{1}{t^s}$ mit Hülfe der Ungleichung $\frac{1}{n_{t'}}<\frac{h\varkappa+\delta}{t'}$ die Convergenz der Reihe

$$\sum_{(t)}\frac{1}{n_t^s}=\sum_{(\mathfrak{j})}\frac{1}{n(\mathfrak{j})^s}$$

für $s>1$, wo t alle ganzen positiven Zahlen und $\mathfrak{j}$ alle Ideale des Körpers k durchläuft. Ferner ergiebt sich aus den Ungleichungen (14) die Formel:

$$(h\varkappa-\delta)^s(s-1)\sum_{(t')}\frac{1}{t'^s} < (s-1)\sum_{(t')}\frac{1}{n_{t'}^s} < (h\varkappa+\delta)^s(s-1)\sum_{(t')}\frac{1}{t'^s},$$

wo die Summen sich über alle ganzzahligen Werte von t' zu erstrecken

haben, welche $\geqq t$ sind. Der Grenzübergang zu $s=1$ liefert:

$$h\varkappa-\delta \leqq \underset{s=1}{L}\left\{(s-1)\sum_{(t')}\frac{1}{n_{t'}^s}\right\} \leqq h\varkappa+\delta.$$

Nun ist

$$\underset{s=1}{L}\left\{(s-1)\sum_{(\mathfrak{j})}\frac{1}{n(\mathfrak{j})^s}\right\} = \underset{s=1}{L}\left\{(s-1)\sum_{(t)}\frac{1}{n_t^s}\right\} = \underset{s=1}{L}\left\{(s-1)\sum_{(t')}\frac{1}{n_{t'}^s}\right\}$$

ebenfalls $\geqq h\varkappa-\delta$ und $\leqq h\varkappa+\delta$ und also, da hierin δ eine beliebig kleine Grösse bedeutet, $=h\varkappa$, womit der gewünschte Nachweis des Satzes 56 erbracht ist.

§ 27.

Andere unendliche Entwickelungen der Function $\zeta(s)$.

Die Function $\zeta(s)$ kann noch auf drei andere Arten durch unendliche Entwickelungen dargestellt werden [*Dedekind*[1]]. Es ist, wie leicht ersichtlich:

$$\begin{aligned}\zeta(s) &= \sum_{(n)}\frac{F(n)}{n^s},\\ &= \prod_{(\mathfrak{p})}\frac{1}{1-n(\mathfrak{p})^{-s}},\\ &= \prod_{(p)}\left(\frac{1}{1-p^{-f_1 s}}\,\frac{1}{1-p^{-f_2 s}}\cdots\frac{1}{1-p^{-f_e s}}\right);\end{aligned}$$

hier ist im ersten Ausdruck die Summe über alle ganzen rationalen positiven Werte von n, im zweiten Ausdruck ist das Product über alle Primideale $\mathfrak{p}$ des Körpers k, und im dritten Ausdruck ist das Product über alle rationalen Primzahlen zu erstrecken, wobei $f_1, f_2, \ldots, f_e$ die Grade der e in p aufgehenden Primideale bedeuten. Alle diese unendlichen Summen und Producte für $\zeta(s)$ convergiren für $s>1$, da die Glieder sämtlich positiv sind, in einer von der Reihenfolge der Summanden oder Factoren unabhängigen Weise.

§ 28.

Die Zusammensetzung der Idealklassen eines Körpers.

Betreffs der multiplicativen Darstellung der Idealklassen gilt der folgende wichtige Satz [*Schering*[1], *Kronecker*[11]]:

Satz 57. Es giebt stets q Klassen $A_1, \ldots, A_q$, so dass jede andere Klasse A auf eine und nur auf eine Weise in der Gestalt

$A = A_1^{x_1}, \ldots, A_q^{x_q}$ darstellbar ist; dabei durchlaufen $x_1, \ldots, x_q$ die ganzen Zahlen $0, 1, 2, \ldots$ bez. bis $h_1 - 1, \ldots, h_q - 1$, und es ist $A_1^{h_1} = 1, \ldots, A_q^{h_q} = 1$ und $h = h_1 \ldots h_q$.

Beweis. Man bilde für jede Klasse A den niedrigsten positiven Exponenten e_1 derart, dass $A^{e_1} = 1$ wird. Der grösste aller dieser Exponenten e_1 werde mit h_1 bezeichnet, und es sei H_1 eine hierbei auf h_1 führende Klasse. Nun bestimme man für jede Klasse A den niedrigsten Exponenten e_2 derart, dass A^{e_2} gleich einer Potenz von H_1 wird. Der höchste dieser Exponenten e_2 werde mit h_2 bezeichnet, und H_2 sei eine auf h_2 führende Klasse. Ferner bestimme man für jede Klasse A den niedrigsten Exponenten $e_3 > 0$ derart, dass A^{e_3} gleich einem Product von Potenzen der Klassen H_1, H_2 wird; es sei h_3 der höchste dieser Exponenten e_3 und H_3 eine auf h_3 führende Klasse. Fährt man so fort, so entsteht eine Reihe von Klassen $H_1, H_2, \ldots, H_q$, denen, wie man unmittelbar sieht, die Eigenschaft zukommt, dass eine jede Klasse A auf eine und nur auf eine Weise in der Gestalt $A = H_1^{x_1} \ldots H_q^{x_q}$ dargestellt werden kann, wo $x_1, \ldots, x_q$ die im Satze 57 angegebenen Werte annehmen.

Es sei nun

$$(15.) \qquad H_s^{h_s} = H_t^{a_t} H_{t-1}^{a_{t-1}} \ldots H_1^{a_1},$$

wo $t < s$ ist und $a_t, a_{t-1}, \ldots, a_1$ gewisse ganzzahlige Exponenten bedeuten. Aus den gemachten Festsetzungen folgt $H_s^{h_t} = H_{t-1}^{b_{t-1}} \ldots H_1^{b_1}$, wo $b_{t-1}, \ldots, b_1$ gewisse ganze Zahlen sind; es muss h_t durch h_s teilbar sein, da im anderen Falle bereits eine niedere als die $h_s$te Potenz von H_s als Product der Klassen $H_t, H_{t-1}, \ldots, H_1$ darstellbar sein würde. Wird $h_t = h_s l_s$ gesetzt, so folgt, dass $H_t^{a_t l_t}$ durch ein Product der Klassen $H_{t-1}, \ldots, H_1$ darstellbar ist; es ist daher notwendig $a_t l_t$ durch h_t, d. h. a_t durch h_s teilbar. Setzen wir $a_t = h_s c_s$ und wählen an Stelle der Klasse H_s die Klasse $H_s' = H_s H_t^{-c_s}$, so geht die Gleichung (15) über in die einfachere Gleichung $H_s'^{h_s} = H_{t-1}^{a_{t-1}} \ldots H_1^{a_1}$. Die Fortsetzung dieses Verfahrens führt schliesslich zu einer Klasse A_s an Stelle von H_s, für welche die gewünschte Relation $A_s^{h_s} = 1$ stattfindet.

Die obige Darstellung der Klassen kann überdies so eingerichtet werden, dass die Zahlen $h_1, \ldots, h_q$ Primzahlen oder Primzahlpotenzen sind. Wäre nämlich g eine der Zahlen $h_1, \ldots, h_r$, welche noch nicht Primzahl oder Primzahlpotenz ist, und wäre etwa $g = p'p'' \ldots$, wo $p', p'', \ldots$ Potenzen verschiedener Primzahlen sind, so setze man,

wenn B die zu g gehörige Klasse bezeichnet, $B' = B^{\frac{g}{p'}}$, $B'' = B^{\frac{g}{p''}}$, ... Wir haben dann $B'^{p'} = 1$, $B''^{p''} = 1$, ..., und wenn

$$\frac{1}{g} = \frac{a'}{p'} + \frac{a''}{p''} + \cdots$$

gesetzt wird, so folgt $B = B'^{a'} B''^{a''} \ldots$. Es kann also B', B'', ... an Stelle von B eingeführt werden. Sind die Klassen $A_1, \ldots, A_q$ in der zuletzt beschriebenen Weise gewählt, so heissen dieselben ein **System von Grundklassen.**

§ 29.

Die Charaktere einer Idealklasse. Eine Verallgemeinerung der Function $\zeta(s)$.

Nachdem ein bestimmtes System von Grundklassen ausgewählt worden ist, ist eine jede vorhandene Klasse A durch die Exponenten $x_1, \ldots, x_q$ und mithin auch durch die q Einheitswurzeln

$$\chi_1(A) = e^{\frac{2i\pi x_1}{h_1}}, \quad \ldots, \quad \chi_r(A) = e^{\frac{2i\pi x_r}{h_r}}$$

eindeutig bestimmt. Diese q Einheitswurzeln $\chi(A)$ heissen die **Charaktere der Klasse** A. Sind $\chi(A)$, $\chi(B)$ Charaktere der beiden Klassen A, bez. B, so ist offenbar $\chi(AB) = \chi(A)\chi(B)$. Der Charakter $\chi(A)$ einer Klasse wird zugleich auch als der Charakter $\chi(\mathfrak{a})$ eines jeden in A enthaltenen Ideals $\mathfrak{a}$ bezeichnet.

Mit Hülfe eines Charakters χ lässt sich dann eine Function bilden, welche eine Verallgemeinerung der oben betrachteten Function $\zeta(s)$ ist, und welche eine ähnliche Productentwickelung gestattet [*Dedekind*[1]]. Diese Function ist

$$\sum_{(\mathfrak{j})} \frac{\chi(\mathfrak{j})}{n(\mathfrak{j})^s} = \prod_{(\mathfrak{p})} \frac{1}{1 - \chi(\mathfrak{p})\, n(\mathfrak{p})^{-s}},$$

wo die Summe über alle Ideale $\mathfrak{j}$ und das Product über alle Primideale $\mathfrak{p}$ des Körpers k zu erstrecken ist.

Capitel VIII.

Die zerlegbaren Formen des Körpers.

§ 30.

Die zerlegbaren Formen des Körpers. Die Formenklassen und ihre Zusammensetzung.

Wenn $\xi^{(1)}, \ldots, \xi^{(m)}$ m lineare Formen der m Veränderlichen $u_1, \ldots, u_m$ mit beliebigen reellen oder imaginären Coefficienten sind, so heisst das Product

$$U(u_1, \ldots, u_m) = \xi^{(1)} \ldots \xi^{(m)}$$

eine **zerlegbare Form** $m$ten Grades der m Veränderlichen $u_1, \ldots, u_m$. Die Coefficienten der Producte von $u_1, \ldots, u_m$ heissen die **Coefficienten der Form.** Berücksichtigt man die Formeln

$$-\frac{\partial^2 \log U}{\partial u_r \partial u_s} = \frac{\partial \log \xi^{(1)}}{\partial u_r}\frac{\partial \log \xi^{(1)}}{\partial u_s} + \cdots + \frac{\partial \log \xi^{(m)}}{\partial u_r}\frac{\partial \log \xi^{(m)}}{\partial u_s},$$
$$(r, s = 1, \ldots, m)$$

so folgt leicht aus dem Multiplicationssatz der Determinanten, dass das Quadrat der Determinante der m linearen Formen $\xi^{(1)}, \ldots, \xi^{(m)}$ gleich $(-1)^m U^2 \Sigma \pm \frac{\partial^2 \log U}{\partial u_1 \partial u_1} \cdots \frac{\partial^2 \log U}{\partial u_m \partial u_m}$ und daher eine ganze ganzzahlige Function der Coefficienten von U ist; dasselbe werde die **Discriminante der Form** U genannt. Eine Form U, deren Coefficienten ganze rationale Zahlen ohne gemeinsamen Teiler sind, heisst eine **primitive Form;** dieselbe ist eine rationale Einheitsform.

Sind $\alpha_1, \ldots, \alpha_m$ eine Basis des Ideals $\mathfrak{a}$, so ist insbesondere die Norm $n(\xi) = n(\alpha_1 u_1 + \cdots + \alpha_m u_m)$ eine zerlegbare Form $m$ten Grades. Die Coefficienten derselben sind ganze rationale Zahlen mit dem grössten gemeinsamen Teiler $n(\mathfrak{a})$. Nach Forthebung dieses Teilers entsteht eine primitive Form U, welche eine **zerlegbare Form des Körpers** k genannt wird, und welche folgende Eigenschaften besitzt. Wählt man an Stelle der Basis $\alpha_1, \ldots, \alpha_m$ eine andere Basis $\alpha_1^*, \ldots, \alpha_m^*$ des Ideals $\mathfrak{a}$, so erhält man eine Form U^*, welche aus U vermöge ganzzahliger linearer Transformation von der Determinante ± 1 hervorgeht. Fasst man alle diese transformirten Formen unter den Begriff der **Formenklasse** zusammen, so ist ersichtlich, dass einem jeden Ideal $\mathfrak{a}$ eine bestimmte Formenklasse

zugehört. Die nämliche Formenklasse entsteht offenbar auch, wenn man statt des Ideals $\mathfrak{a}$ das Ideal $\alpha\mathfrak{a}$ zu Grunde legt, wo α eine ganze oder gebrochene Zahl des Körpers bedeutet, d. h. einem jedem Ideal der nämlichen Idealklasse entspricht die nämliche Formenklasse.

Da die Discriminante der Form $n(\xi) = n(\mathfrak{a})U$ offenbar gleich $n(\mathfrak{a})^2 d$ ist, so folgt die Thatsache:

Satz 58. Die Discriminante einer zerlegbaren Form U des Körpers k ist gleich der Körperdiscriminante d. [*Dedekind*[1].]

Die genannten Eigenschaften der Formen U bestimmen das Wesen derselben vollständig; es gilt nämlich der umgekehrte Satz:

Satz 59. Wenn U eine primitive, im Körper k zerlegbare, aber in jedem Körper niederen Grades unzerlegbare Form $m$ten Grades mit der Discriminante d des Körpers ist, so giebt es in k mindestens eine und höchstens m Idealklassen, denen die Form U zugehört.

Beweis. Ist etwa $\eta = \mu_1 u_1 + \cdots + \mu_m u_m$ ein Linearfactor von U, dessen Coefficienten in k liegen, so multiplicire man ξ mit einer ganzen Zahl α derart, dass $\xi = \alpha\eta = \alpha_1 u_1 + \cdots + \alpha_m u_m$ eine lineare Form mit ganzen Coefficienten $\alpha_1, \ldots, \alpha_m$ wird. Setzen wir $\mathfrak{a} = (\alpha_1, \ldots, \alpha_m)$, so ist nach Satz 20 $n(\xi) = n(\mathfrak{a})U$, und da die Discriminante der Form U gleich der Körperdiscriminante sein soll, so ergiebt sich hieraus:

$$\begin{vmatrix} \alpha_1', & \ldots, & \alpha_m' \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot \\ \alpha_1^{(m-1)}, & \ldots, & \alpha_m^{(m-1)} \end{vmatrix}^2 = n(\mathfrak{a})^2 d,$$

wo die gestrichenen α bez. die conjugirten Zahlen bedeuten. Aus dieser Gleichung folgt, wenn wir die Umkehrung des Satzes 19 zu Hülfe nehmen, dass $\alpha_1, \ldots, \alpha_m$ eine Basis des Ideals $\mathfrak{a}$ bilden.

Gehören zu den beiden Idealen $\mathfrak{a}$, $\mathfrak{b}$ bezüglich die beiden Formen U, V, so heisst jede zu dem Ideale $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ gehörige Form W eine aus den Formen U und V **zusammengesetzte Form.** [*Dedekind*[1].]

Die Entscheidung der Frage, ob zwei vorgelegte, zum Körper k gehörige Formen zu derselben oder zu verschiedenen Formenklassen gehören, kommt, der obigen Entwickelung zufolge, auf die Frage nach der Aequivalenz zweier vorgelegter Ideale hinaus und erfordert daher zu ihrer Entscheidung nur eine endliche Anzahl von Operationen. Vgl. § 24.

Capitel IX.

Die Zahlringe des Körpers.

§ 31.

Der Zahlring. Das Ringideal und seine wichtigsten Eigenschaften.

Sind ϑ, η, ... irgend welche ganze algebraische Zahlen, deren Rationalitätsbereich der Körper k vom $m$ten Grade ist, so wird das System aller ganzen Functionen von ϑ, η, ..., deren Coefficienten ganze rationale Zahlen sind, ein **Zahlring, Ring** oder **Integritätsbereich***) genannt. Die Addition, Subtraction und Multiplication zweier Zahlen eines Ringes liefert wiederum eine Zahl des Ringes. Der Begriff des Ringes ist mithin gegenüber den drei Rechnungsoperationen der Addition, Subtraction und Multiplication invariant. Der grösste Zahlring des Körpers k ist der durch $\omega_1, \ldots, \omega_m$ bestimmte Ring, wo $\omega_1, \ldots, \omega_m$ die Zahlen einer Körperbasis bedeuten. Derselbe umfasst alle ganzen Zahlen des Körpers. Jeder Zahlring r enthält m ganze Zahlen $\varrho_1, \ldots, \varrho_m$ von der Art, dass jede andere Zahl ϱ des Ringes in der Gestalt

$$\varrho = a_1\varrho_1 + \cdots + a_m\varrho_m$$

dargestellt werden kann, wo $a_1, \ldots, a_m$ ganze rationale Zahlen sind. Die Zahlen $\varrho_1, \ldots, \varrho_m$ heissen eine **Basis des Ringes.** Bezeichnen wir die zu $\varrho_1, \ldots, \varrho_m$ conjugirten Zahlen bez. mit $\varrho'_1, \ldots, \varrho'_m, \ldots, \varrho_1^{(m-1)}, \ldots, \varrho_m^{(m-1)}$, so ist das Quadrat der Determinante

$$\begin{vmatrix} \varrho_1, & \ldots, & \varrho_m \\ \varrho'_1, & \ldots, & \varrho'_m \\ \cdot & \cdot & \cdot \\ \varrho_1^{(m-1)}, & \ldots, & \varrho_m^{(m-1)} \end{vmatrix}$$

eine rationale Zahl und heisst die **Discriminante** d_r **des Ringes** r.

Ein **Ringideal** oder ein **Ideal des Ringes** r wird ein solches unendliches System von ganzen algebraischen Zahlen $\alpha_1, \alpha_2, \ldots$ des Ringes r genannt, welches die Eigenschaft besitzt, dass eine jede lineare Combination $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \cdots$ derselben wiederum dem System angehört,

*) Nach *Dedekind* „eine Ordnung“.

wobei die Coefficienten λ_1, λ_2, ... beliebige Zahlen des Ringes r sind. Jedes Ringideal enthält m ganze Zahlen $\iota_1, \ldots, \iota_m$ von der Art, dass eine jede Zahl des Ringideals gleich einer linearen Combination derselben von der Gestalt $a_1\iota_1 + \cdots + a_m\iota_m$ ist, wo $a_1, \ldots, a_m$ ganze rationale Zahlen bedeuten. Die Zahlen $\iota_1, \ldots, \iota_m$ heissen eine **Basis des Ringideals.** Der Beweis für die Existenz einer Basis des Ringes und des Ringideals ist genau entsprechend den in § 3 und § 4 dargelegten Beweisen für die Existenz der Körperbasis und Idealbasis zu führen. Es gelten folgende Sätze: [*Dedekind*[3].]

Satz 60. Sind $\iota_1, \ldots, \iota_m$ irgend m ganze Zahlen des Körpers k, zwischen denen keine lineare Relation mit ganzen rationalen Zahlencoefficienten besteht, so giebt es stets einen Ring r, in welchem $\iota_1, \ldots, \iota_m$ die Basis eines Ringideals bilden.

Beweis. Es sei ϱ eine beliebige ganze Zahl des Körpers, für welche die m Zahlen $\varrho\iota_1, \ldots, \varrho\iota_m$ sämtlich gleich linearen Combinationen der Zahlen $\iota_1, \ldots, \iota_m$ von der Gestalt $a_1\iota_1 + \cdots + a_m\iota_m$ werden, wo $a_1, \ldots, a_m$ ganze rationale Zahlen sind. Die Gesamtheit aller dieser ganzen Zahlen ϱ des Körpers bestimmt, wie leicht einzusehen, einen Ring von der verlangten Beschaffenheit.

Sind $\alpha_1, \ldots, \alpha_s$ irgend s Zahlen in r, durch deren lineare Combination unter Benutzung ganzer algebraischer, in r liegender Coefficienten alle Zahlen eines Ringideals $\mathfrak{j}_r$ erhalten werden können, so setzen wir kurz $\mathfrak{j}_r = [\alpha_1, \ldots, \alpha_s]$. Insbesondere ist $\mathfrak{j}_r = [\iota_1, \ldots, \iota_m]$.

Satz 61. Es giebt in jedem Ringe r stets Ringideale $\mathfrak{j}_r$, welche zugleich Körperideale sind.

Beweis. Drückt man $\omega_1, \ldots, \omega_m$ durch die Zahlen $\varrho_1, \ldots, \varrho_m$ der Basis des Ringes r aus, in der Gestalt

$$\omega_i = \frac{a_{i1}\varrho_1 + \cdots + a_{im}\varrho_m}{A}, \qquad (i = 1, 2, \ldots, m)$$

wo $a_{i1}, \ldots, a_{im}$, A ganze rationale Zahlen sind, so folgt, dass jede durch A teilbare ganze Zahl in k eine Zahl des Ringes und mithin jedes durch A teilbare Ideal des Körpers k zugleich ein Ringideal des Ringes r ist.

Der grösste gemeinsame Idealteiler aller derjenigen Körperideale, welche zugleich Ringideale in r sind, heisst der **Führer $\mathfrak{f}$ des Ringes** r. [*Dedekind*[3].] Es folgt dann leicht der Satz:

Satz 62. Jedes durch den Führer $\mathfrak{f}$ teilbare Ideal $\mathfrak{j}$ des Körpers k ist zugleich ein Ringideal des Ringes r.

§ 32.
Die durch eine ganze Zahl bestimmten Ringe. Der Satz von der Differente einer ganzen Zahl des Körpers.

Die wichtigsten Zahlringe des Körpers sind diejenigen, welche durch eine einzige ganze Zahl ϑ bestimmt werden. Auf die Eigenschaften dieser besonderen Zahlringe hat *Dedekind* seine Theorie der Discriminanten algebraischer Zahlkörper gegründet [*Dedekind*[6]]. Die hauptsächlichsten Resultate von *Dedekind* fassen wir in folgenden Satz zusammen:

Satz 63. Der grösste gemeinsame Teiler der Differenten aller ganzen Zahlen des Körpers k ist gleich der Differente $\mathfrak{d}$ des Körpers. Ist δ die Differente einer ganzen Zahl ϑ, welche den Körper k bestimmt, und $\mathfrak{f}$ der Führer des durch ϑ bestimmten Zahlringes, so ist $\delta = \mathfrak{f}\mathfrak{d}$.

Beweis. Es sei $\omega_1, \ldots, \omega_m$ eine Körperbasis von k, und es seien bezüglich $\omega'_1, \ldots, \omega'_m, \ldots, \omega_1^{(m-1)}, \ldots, \omega_m^{(m-1)}$ die zu diesen m Zahlen conjugirten Zahlen. Wir bilden die m-reihige Determinante der m^2 Zahlen $\omega_h^{(l)}$:

$$\Omega = \begin{vmatrix} \omega_1, & \ldots, & \omega_m \\ \omega'_1, & \ldots, & \omega'_m \\ \cdot & \cdot & \cdot \\ \omega_1^{(m-1)}, & \ldots, & \omega_m^{(m-1)} \end{vmatrix}$$

und bezeichnen die zu $\omega_1, \ldots, \omega_m$ adjungirten $(m-1)$-reihigen Unterdeterminanten von Ω bezüglich mit $\Omega_1, \ldots, \Omega_m$. Die m Producte $\Omega\Omega_1, \ldots, \Omega\Omega_m$ sind dann ganze Zahlen des Körpers k, und zwar bilden dieselben die Basiszahlen eines Ideals des Körpers k.

Um das letztere zu beweisen, multipliciren wir die $m-1$ Horizontalreihen der Determinante Ω_h bezüglich mit

$$(16) \qquad u+\omega'_i, \quad u+\omega''_i, \quad \ldots, \quad u+\omega_i^{(m-1)},$$

wo u ein unbestimmter Parameter ist. Die entstehende $(m-1)$-reihige Determinante erhält dann, wie leicht ersichtlich, die Gestalt:

$$f_1(u)\Omega_1 + f_2(u)\Omega_2 + \cdots + f_m(u)\Omega_m,$$

wo $f_1, \ldots, f_m$ ganzzahlige Functionen von u sind. Andererseits hat das Product der $m-1$ Linearfactoren (16) die Form

$$u^{m-1} + (\omega'_i + \cdots + \omega_i^{(m-1)})u^{m-2} + \cdots = u^{m-1} + (a - \omega_i)u^{m-2} + \cdots,$$

wo a eine ganze rationale Zahl bedeutet. Die Vergleichung der Coef-

ficienten von u^{m-2} liefert das Resultat, dass $\omega_i \boldsymbol{\Omega}_h$ eine lineare Combination von $\boldsymbol{\Omega}_1, \ldots, \boldsymbol{\Omega}_m$ mit ganzen rationalen Zahlencoefficienten ist; hiermit ist der gewünschte Nachweis dafür geführt, dass $\boldsymbol{\Omega}\boldsymbol{\Omega}_1, \ldots, \boldsymbol{\Omega}\boldsymbol{\Omega}_m$ Basiszahlen eines Ideals sind.

Bezeichnen wir allgemein mit $\boldsymbol{\Omega}_h^{(l)}$ die zu $\omega_h^{(l)}$ adjungirte $(m-1)$-reihige Unterdeterminante der Determinante $\boldsymbol{\Omega}$, so wird nach einem bekannten Determinantensatze die m-reihige Determinante $|\boldsymbol{\Omega}_h^{(l)}| = \boldsymbol{\Omega}^{m-1}$; folglich genügt die Norm des Ideals $\mathfrak{J} = (\boldsymbol{\Omega}\boldsymbol{\Omega}_1, \ldots, \boldsymbol{\Omega}\boldsymbol{\Omega}_m)$ der Gleichung

$$dn^2(\mathfrak{J}) = |\boldsymbol{\Omega}\boldsymbol{\Omega}_h^{(l)}|^2 = \boldsymbol{\Omega}^{4m-2},$$

und hieraus folgt $n(\mathfrak{J}) = |d|^{m-1}$. Nun ist offenbar die Discriminante d des Körpers durch $\mathfrak{J}$ teilbar; setzen wir $d = \mathfrak{J}\mathfrak{j}$, so folgt $n(\mathfrak{j}) = |d|$.

Es sei nun ϑ irgend eine den Körper k bestimmende Zahl; dann können wir die m Basiszahlen des Körpers k in der Gestalt voraussetzen:

$$\begin{aligned}
\omega_1 &= 1,\\
\omega_2 &= \frac{a_1 + \vartheta}{f_1},\\
\omega_3 &= \frac{a_2 + a_2'\vartheta + \vartheta^2}{f_2},\\
&\cdots\cdots\cdots\\
\omega_m &= \frac{a_{m-1} + a_{m-1}'\vartheta + \cdots + a_{m-1}^{(m-2)}\vartheta^{m-2} + \vartheta^{m-1}}{f_{m-1}},
\end{aligned}$$

wo $a_1, a_2, a_2', \ldots, a_{m-1}^{(m-2)}, f_1, \ldots, f_{m-1}$ ganze rationale Zahlen sind. Wir ermitteln nun den Führer $\mathfrak{f}$ des durch ϑ bestimmten Ringes und stellen die Basiszahlen desselben in der Gestalt dar:

$$\begin{aligned}
\varrho_1 &= f_1',\\
\varrho_2 &= b_1 + f_2'\vartheta,\\
\varrho_3 &= b_2 + b_2'\vartheta + f_3'\vartheta^2,\\
&\cdots\cdots\cdots\\
\varrho_m &= b_{m-1} + b_{m-1}'\vartheta + \cdots + b_{m-1}^{(m-2)}\vartheta^{m-2} + f_m'\vartheta^{m-1},
\end{aligned}$$

wo $b_1, b_2, b_2', \ldots, b_{m-1}^{(m-2)}, f_1', f_2', \ldots, f_m'$ ganze rationale Zahlen bedeuten. Da insbesondere nach Satz 62 $\varrho_1\omega_m, \varrho_2\omega_{m-1}, \ldots, \varrho_m\omega_1$ ganzzahlige Functionen von ϑ werden müssen, so ergiebt sich notwendigerweise, dass f_1' durch f_{m-1}, f_2' durch $f_{m-2}, \ldots, f_{m-1}'$ durch f_1 und folglich das Product

$f'_1 \cdots f'_{m-1}$ durch das Product $f = f_1 \cdots f_{m-1}$ teilbar sein muss. Da $n(\mathfrak{f}) = f_1 \cdots f_{m-1} f'_1 \cdots f'_{m-1} f'_m$ ist, so wird $n(\mathfrak{f}) = f^2 g$, wo g eine ganze rationale Zahl ist.

Wir setzen ferner:

$$\Theta = \begin{vmatrix} 1, & \vartheta & , \ldots, & \vartheta^{m-1} \\ 1, & \vartheta' & , \ldots, & \vartheta'^{m-1} \\ \cdot & \cdot & \cdot & \cdot \\ 1, & \vartheta^{(m-1)}, & \ldots, & (\vartheta^{(m-1)})^{m-1} \end{vmatrix}, \quad H = (-1)^{\frac{m-1}{2}} \begin{vmatrix} 1, & \vartheta', & \ldots, & \vartheta'^{m-2} \\ \cdot & \cdot & \cdot & \cdot \\ 1, & \vartheta^{(m-1)}, & \ldots, & (\vartheta^{(m-1)})^{m-2} \end{vmatrix};$$

es gelten dann für die Differente δ der Zahl ϑ die Beziehungen $(-1)^{m-1}\delta = \frac{\Theta}{H}$ und nach S. 180 $(-1)^{\frac{m(m-1)}{2}} n(\delta) = \Theta^2 = f^2 d$. Ferner ist

$$(17.) \begin{cases} \sum\limits_{(h=1,\ldots,m)} u_h \Omega \Omega_h \\ = \frac{\Theta}{f^2} \begin{vmatrix} u_1, f_1 u_2, & f_2 u_3, & , \ldots, f_{m-1} u_m \\ 1, a_1 + \vartheta', & a_2 + a'_2 \vartheta' + \vartheta'^2, & , \ldots, a_{m-1} + \cdots + \vartheta'^{m-1} \\ \cdot & \cdot & \cdot \\ 1, a_1 + \vartheta^{(m-1)}, & a_2 + a'_2 \vartheta^{(m-1)} + (\vartheta^{(m-1)})^2, & \ldots, a_{m-1} + \cdots + (\vartheta^{(m-1)})^{m-1} \end{vmatrix}, \end{cases}$$

wo $u_1, \ldots, u_m$ Unbestimmte sind. Entwickeln wir hier die Determinante nach den Elementen der ersten Horizontalreihe und schreiben sie dabei in der Gestalt $u_1 H_1 + \cdots + u_m H_m$, so sind, wie man leicht erkennt, die Zahlen $\frac{H_1}{H}, \ldots, \frac{H_m}{H}$ sämtlich ganze Zahlen des Körpers k; sie gehen, wie die Formel (17.) zeigt, aus den Zahlen $\Omega\Omega_1, \ldots, \Omega\Omega_m$ dadurch hervor, dass man die letzteren mit ein und demselben in k liegenden Factor multiplicirt. Die m Zahlen $\frac{H_1}{\Theta_1}, \ldots, \frac{H_m}{\Theta_1}$ sind folglich wieder Basiszahlen eines Ideals $\mathfrak{m}$; dieses Ideal heisse $\mathfrak{m}$.

Die Zahlen des Ideals $\mathfrak{m}$ sind sämtlich ganzzahlige Functionen von ϑ. Dasselbe ist folglich durch $\mathfrak{f}$ teilbar, und wir setzen $\mathfrak{m} = \mathfrak{f}\mathfrak{l}$, wo $\mathfrak{l}$ ein gewisses Ideal in k bedeutet. Unsere Gleichung (17.) zeigt dann, dass

$$\mathfrak{J} = \frac{\Theta H}{f^2} \mathfrak{f}\mathfrak{l} = \frac{d\mathfrak{f}\mathfrak{l}}{\mathfrak{d}}$$

ist, und wenn man die Norm nimmt, so folgt hieraus:

$$|d|^{m-1} = \frac{|d|^m n(\mathfrak{f}) n(\mathfrak{l})}{f^2 |d|}, \quad \text{d. h.} \quad f^2 = n(\mathfrak{f}) n(\mathfrak{l}).$$

Da andererseits vorhin $n(\mathfrak{f}) = f^2 g$ gefunden worden ist, so muss $g = 1$, $n(\mathfrak{l}) = 1$, $\mathfrak{l} = 1$ sein, und folglich wird $n(\mathfrak{f}) = f^2$, $\mathfrak{J}\delta = \mathfrak{f}d$, $\delta = \mathfrak{f}\mathfrak{j}$.

Nunmehr sei $\mathfrak{p}$ ein beliebig gegebenes Primideal des Körpers k, so beweisen wir zunächst, dass sich stets eine ganze Zahl $\vartheta = \varrho$ in k finden lässt von der Art, dass der Führer des durch ϱ bestimmten Ringes nicht durch $\mathfrak{p}$ teilbar ist. Es sei die durch $\mathfrak{p}$ teilbare rationale Primzahl $p = \mathfrak{p}^e \mathfrak{a}$, wo $\mathfrak{a}$ ein zu $\mathfrak{p}$ primes Ideal bedeutet; ferner sei ϱ als ganze Zahl in k derart ausgewählt, dass jede beliebige ganze Zahl des Körpers k nach jeder noch so hohen Potenz von $\mathfrak{p}$ congruent einer ganzzahligen Function von ϱ wird. Die Existenz einer solchen Zahl ϱ ist in Satz 29 gezeigt worden; zugleich werde die Zahl ϱ so gewählt, dass sie $\equiv 0$ nach $\mathfrak{a}$ wird (Satz 25) und eine den Körper k bestimmende Zahl ist. Nunmehr sei die Discriminante $d(\varrho)$ der Zahl ϱ gleich $p^h a$, wo a eine zu p prime, ganze rationale Zahl bedeutet. Es ist dann jede ganze Zahl ω des Körpers k in der Gestalt $\omega = \frac{F(\varrho)}{a\varrho^h}$ darstellbar, wo $F(\varrho)$ eine ganze ganzzahlige Function von ϱ bezeichnet. In der That: wird $\omega \equiv H(\varrho)$ nach $\mathfrak{p}^{eh}$, wo $H(\varrho)$ eine ganzzahlige Function von ϱ bedeutet, und setzen wir $\omega = H(\varrho) + \omega^*$, so folgt, dass $\omega^* \varrho^h$ durch p^h teilbar wird. Wir setzen $\omega^* \varrho^h = p^h \alpha$, wo α eine ganze Zahl des Körpers k bedeutet. Da nach § 3 eine jede ganze Zahl α in die Gestalt $\frac{G(\varrho)}{d(\varrho)}$ gebracht werden kann, wo $G(\varrho)$ eine ganze ganzzahlige Function von ϱ bedeutet, so folgt $\omega^* = \frac{G(\varrho)}{a\varrho^h}$ und weiter $\omega = \frac{a\varrho^h H(\varrho) + G(\varrho)}{a\varrho^h}$. Die eben gefundene Eigenschaft der Zahl ϱ lehrt, dass die Zahl $a\varrho^h$ jedenfalls in dem Führer des durch ϱ bestimmten Ringes vorkommt. Derselbe ist mithin nicht durch $\mathfrak{p}$ teilbar, d. h. die Zahl $\varrho = \vartheta$ ist eine Zahl von der oben verlangten Beschaffenheit.

Die letzten Entwickelungen zeigen, dass das Ideal $\mathfrak{j}$ genau der grösste gemeinsame Teiler der Differenten aller ganzen Zahlen ist. Andererseits enthält dieser grösste gemeinsame Teiler, wie aus der Definition der Körperdifferente $\mathfrak{d}$ folgt, notwendig dieses Ideal $\mathfrak{d}$ als Factor; wir setzen $\mathfrak{j} = \mathfrak{h}\mathfrak{d}$. Da $n(\mathfrak{d})$ nach Satz 13 durch die Discriminante d teilbar ist, so folgt $n(\mathfrak{j}) = n(\mathfrak{h}) d a$, wo a eine ganze rationale Zahl bedeutet. Wegen $n(\mathfrak{j}) = \pm d$ folgt hieraus $n(\mathfrak{h}) = 1$, $\mathfrak{h} = 1$, $a = \pm 1$, also $\mathfrak{j} = \mathfrak{d}$. Damit ist der Satz 63 vollständig bewiesen.

Aus dem Satze 63 folgen leicht der Satz 31 und 37, sowie die am Schluss des § 12 aufgestellte Behauptung über die in der Discriminante des Körpers aufgehenden Primzahlen. Um die letztere abzuleiten, hat man nur nötig, die Zerlegung der linken Seite der Gleichung, welcher $\vartheta = \varrho$ genügt, nach der betreffenden Primzahl p vorzunehmen und in ähnlicher Weise zu verwerthen, wie dies in § 11 für die linke Seite der Fundamentalgleichung geschehen ist.

§ 33.

Die regulären Ringideale und ihre Teilbarkeitsgesetze.

Ist ein beliebiger Ring r und in ihm ein Ringideal $\mathfrak{j}_r = [\alpha_1, \ldots, \alpha_s]$ gegeben, so hat man in dem grössten gemeinsamen Idealteiler der Zahlen des letzteren ein Körperideal; wir nennen dieses Ideal $\mathfrak{j} = (\alpha_1, \ldots, \alpha_s)$ das dem Ringideal $\mathfrak{j}_r$ **zugeordnete Körperideal.** Wenn insbesondere das Körperideal $\mathfrak{j}$ zum Führer $\mathfrak{f}$ des Ringes r prim ist, so heisse $\mathfrak{j}_r$ ein **reguläres Ringideal.** Es gilt der Satz:

Satz 64. Wenn $\mathfrak{j}$ ein beliebiges zu dem Führer $\mathfrak{f}$ primes Körperideal ist, so existirt im Ringe r stets ein Ringideal $\mathfrak{j}_r$, dem das Körperideal $\mathfrak{j}$ zugeordnet ist.

Beweis. Wir bestimmen das System aller der Zahlen des Ringes r, welche durch das gegebene Körperideal $\mathfrak{j}$ teilbar sind. Dieselben bilden in r ein Ringideal $\mathfrak{j}_r = [\alpha_1, \ldots, \alpha_s]$. Ferner wählen wir in dem Führer $\mathfrak{f}$ des Ringes r eine zu $\mathfrak{j}$ prime ganze Zahl φ und dann im Körperideal $\mathfrak{j}$ eine zu φ prime Zahl α. Alsdann giebt es stets ganze Zahlen ψ und β des Körpers derart, dass $\varphi\psi + \alpha\beta = 1$ wird. Da $\varphi\psi$ durch $\mathfrak{f}$ teilbar und daher eine Zahl des Ringes r ist, so liegt auch $\alpha\beta$ im Ringe r, und da andererseits $\alpha\beta$ durch $\mathfrak{j}$ teilbar ist, so stellt $\alpha\beta = 1 - \varphi\psi$ eine Zahl des Ringideals $\mathfrak{j}_r$ dar: das dem Ringideal $\mathfrak{j}_r$ zugeordnete Körperideal $\mathfrak{j} = (\alpha_1, \ldots, \alpha_s)$ ist folglich zu $\mathfrak{f}$ prim.

Unter dem **Product zweier Ringideale** $\mathfrak{a}_r = [\alpha_1, \ldots, \alpha_s]$ und $\mathfrak{b}_r = [\beta_1, \ldots, \beta_t]$ wird das Ringideal

$$\mathfrak{a}_r \mathfrak{b}_r = [\alpha_1\beta_1, \ \ldots, \ \alpha_s\beta_1, \ \ldots, \ \alpha_1\beta_t, \ \ldots, \ \alpha_s\beta_t]$$

verstanden. Es ist dann der Satz unmittelbar ersichtlich:

Satz 65. Dem Product zweier regulärer Ringideale ist stets das Product der zugeordneten Körperideale zugeordnet.

Vermöge dieses Satzes 65 entsprechen die Teilbarkeits- und Zerlegungs-

gesetze der regulären Ringideale vollkommen den Gesetzen über die Teilbarkeit und Zerlegung der zu $\mathfrak{f}$ primen Körperideale.

Da wir im Folgenden nur reguläre Ringideale betrachten, so lassen wir der Kürze halber den Zusatz „regulär" fort, so dass von nun an unter einem **Ringideal** stets ein reguläres Ringideal verstanden wird.

Es ist aus Satz 23 zu entnehmen, dass in dem Körper k stets $\varphi(\mathfrak{f})$ nach dem Ideal $\mathfrak{f}$ incongruente, zu $\mathfrak{f}$ prime ganze Zahlen vorhanden sind. Wenn eine von diesen dem Ringe r angehört, so liegen offenbar auch alle diejenigen Zahlen im Ringe r, welche dieser Zahl nach dem Führer $\mathfrak{f}$ congruent sind. Die Anzahl der nach $\mathfrak{f}$ incongruenten und zu $\mathfrak{f}$ primen dem Ringe r angehörigen Zahlen ist ein Teiler von $\varphi(\mathfrak{f})$ und werde mit $\varphi_r(\mathfrak{f})$ bezeichnet.

Unter der **Norm** $n(\mathfrak{a}_r)$ **eines Ringideals** $\mathfrak{a}_r$ versteht man die Norm des dem Ringideal zugeordneten Körperideals $\mathfrak{a}$. Die elementaren Sätze über Normen von Ringidealen sind mit dieser Definition gegeben.

§ 34.

Die Einheiten eines Ringes. Die Ringklassen.

Auch der Satz von der Existenz der Grundeinheiten ist ohne Schwierigkeit auf einen Ring übertragbar; dieser Satz folgt am einfachsten aus dem entsprechenden Satze für die Einheiten des Körpers, wenn man bedenkt, dass, wie aus Satz 24 folgt, jede Einheit des Körpers durch Erheben in die $\varphi(\mathfrak{f})$te Potenz in eine Einheit des Ringes übergehen muss. Der Satz hat genau die für den Körper k geltende Form des Satzes 47; für die in Satz 47 mit r bezeichnete Anzahl werde hier s geschrieben. Es mögen $\varepsilon_1, \ldots, \varepsilon_s$ ein System von s Grundeinheiten des Ringes r bedeuten, d. h. ein System von s Einheiten im Ringe r, durch deren Producte unter Zuhülfenahme der Einheitswurzeln des Ringes sich sämtliche Einheiten in r ausdrücken lassen. Dann heisst die positiv genommene Determinante der s ersten Logarithmen zu diesen Einheiten der Regulator R_r des Ringes r. Die Anzahl der im Ringe r gelegenen Einheitswurzeln werde mit w_r bezeichnet. [*Dedekind*[3].]

Zwei Ringideale $\mathfrak{a}$ und $\mathfrak{b}$ heissen einander äquivalent, wenn zwei ganze Zahlen μ und λ existiren, so dass $\mu\mathfrak{a} = \lambda\mathfrak{b}$ ist. Dabei werde der Aequivalenzbegriff hier in der in § 24 erwähnten engeren Fassung genommen und demgemäss die Einschränkung gemacht, dass $\frac{\mu}{\lambda}$ eine positive Norm besitze. Alle einander äquivalenten Ringideale bilden eine **Ring-**

klasse. Ein Ringideal (α), wo α eine zu $\mathfrak{f}$ prime ganze Zahl mit positiver Norm bedeutet, wird ein Hauptringideal, die Klasse dieser die **Hauptringklasse** genannt. Die weiteren Definitionen und die Sätze über die Multiplication der Ringklassen entsprechen genau denjenigen, die in § 22, 28, 29 für die Idealklassen eines Körpers aufgestellt sind; auch folgt ähnlich, wie in § 22 die Endlichkeit der Anzahl der Ringklassen. Die Bestimmung dieser Anzahl kann nach zwei verschiedenen Methoden, nämlich entweder auf einem rein arithmetischen Wege oder mit Verwendung analytischer Hülfsmittel, entsprechend der in § 25 und § 26 dargelegten Weise ausgeführt werden. Das hierbei sich ergebende Resultat ist folgendes [*Dedekind*[3]]:

Satz 66. Sind h und h_r die Anzahlen der Idealklassen des Körpers k bez. des Ringes r, beide für die engere Fassung des Klassenbegriffes, so ist

$$\frac{h_r}{h} = \frac{\varphi(\mathfrak{f})}{\varphi_r(\mathfrak{f})}\,\frac{w_r R}{w R_r}.$$

Auch die Begriffsbildungen des Capitels VIII lassen sich auf den Ring übertragen; wir gelangen so zu dem Begriffe der zu einer Ringklasse gehörigen **zerlegbaren Form.**

§ 35.

Der Modul und die Modulklasse.

Wenn $\mu_1, \ldots, \mu_m$ irgend m ganze Zahlen des Körpers k sind, zwischen denen keine lineare homogene Relation mit ganzen rationalen Coefficienten besteht, so werde das System aller mittelst ganzer rationaler Coefficienten $a_1, \ldots, a_m$ in der Gestalt $a_1\mu_1 + \cdots + a_m\mu_m$ darstellbaren Zahlen ein **Modul** des Körpers k genannt und mit $[\mu_1, \ldots, \mu_m]$ bezeichnet. Der Begriff des Moduls verhält sich mithin gegenüber den Operationen der Addition und Subtraction invariant. Beispiele von Moduln sind das System aller ganzen Zahlen des Körpers k, das Ideal, der Ring, das Ringideal. Zwei Moduln $[\mu_1, \ldots, \mu_m]$ und $[\lambda_1, \ldots, \lambda_m]$ heissen einander **äquivalent,** wenn zwei ganze Zahlen μ und λ existiren, so dass $[\mu\mu_1, \ldots, \mu\mu_m] = [\lambda\lambda_1, \ldots, \lambda\lambda_m]$ ist. Alle einander äquivalenten Moduln bilden eine **Modulklasse.** *Dedekind* nimmt den Begriff des Moduls in seinen Untersuchungen über algebraische Zahlen als Grundlage. [*Dedekind*[1, 3, 6, 9].]

Das Quadrat der Determinante

$$\begin{vmatrix} \mu_1, & \ldots, & \mu_m \\ \mu_1', & \ldots, & \mu_m' \\ \cdot & \cdot & \cdot \\ \mu_1^{(m-1)}, & \ldots, & \mu_m^{(m-1)} \end{vmatrix}$$

ist, wie leicht ersichtlich, eine ganze rationale Zahl und überdies durch die quadrirte Norm des Ideals $\mathfrak{m} = (\mu_1, \ldots, \mu_m)$ teilbar; der Quotient beider Quadrate werde mit ∂ bezeichnet. Bildet man diesen Quotienten für einen beliebigen zu $[\mu_1, \ldots, \mu_m]$ äquivalenten Modul, so ergiebt sich jedesmal der nämliche Werth ∂. Die ganze rationale Zahl ∂ ist mithin für die durch $[\mu_1, \ldots, \mu_m]$ bestimmte Modulklasse charakteristisch und heisst die **Discriminante der Modulklasse.**

Die Begriffe **zerlegbare Form** und **Formenklasse** werden für den Modul entsprechend definirt, wie dies in § 30 für den Körper selbst geschehen ist. [*Dedekind*[3]].

Zweiter Teil.

Der Galois'sche Zahlkörper.

Capitel X.

Die Primideale des Galois'schen Körpers und seiner Unterkörper.

§ 36.

Die eindeutige Zerlegung der Ideale des Galois'schen Körpers in Primideale.

Ein solcher Zahlkörper K, welcher mit den sämtlichen zu ihm conjugirten Körpern übereinstimmt, heisst ein **Galois'scher Körper.** Ist k ein beliebiger Zahlkörper $m$ten Grades, und sind $k', \ldots, k^{(m-1)}$ die zu k conjugirten Körper, so kann aus sämtlichen Zahlen der Körper $k, k', \ldots, k^{(m-1)}$ ein neuer Körper K zusammengesetzt werden; dieser Körper K ist dann notwendig ein Galois'scher Körper, welcher die Körper $k, k', \ldots, k^{(m-1)}$ als Unterkörper enthält. Ein jeder beliebiger Körper k kann mithin stets als ein Körper aufgefasst werden, welcher in einem Galois'schen Körper als Unterkörper enthalten ist. Infolge dieses Umstandes ist es keine wesentliche Einschränkung, wenn wir bei der Erforschung der Eigenschaften der algebraischen Zahlen von vornherein einen Galois'schen Körper zu Grunde legen und dann entwickeln, in welcher Weise die Zerlegungsgesetze für die Ideale dieses Galois'schen Körpers sich auf einen beliebigen in ihm enthaltenen Unterkörper übertragen.

Was zunächst den Beweis für die eindeutige Zerlegung der Ideale in Primideale betrifft, so gestaltet sich derselbe für einen Galois'schen Körper ausserordentlich einfach. [*Hilbert*[1, 2].] Um dies einzusehen, setzen wir zunächst einige Bezeichnungen fest.

Der Galois'sche Körper K vom Mten Grade werde durch die ganze Zahl Θ bestimmt; Θ genügt dann einer irreduciblen Gleichung Mten Grades mit ganzen rationalen Coefficienten. Die M Wurzeln dieser Gleichung seien

$$s_1\Theta = \Theta,\quad s_2\Theta,\quad \ldots,\quad s_M\Theta,$$

wo $s_1, \ldots, s_M$ rationale Functionen von Θ mit rationalen Coefficienten bedeuten. Werden $s_1, \ldots, s_M$ als Substitutionen aufgefasst, so bilden sie eine Gruppe G vom Mten Grade, da ja die auf einander folgende Anwendung irgend zweier von den Substitutionen $s_1, \ldots, s_M$ wiederum eine dieser Substitutionen ergeben muss. G heisse die **Gruppe des Galois'schen Körpers** K. Ein Ideal $\mathfrak{J}$, welches ungeändert bleibt, wenn man die Zahlen desselben durch ihre Conjugirten ersetzt, d. h. wenn man sie einer der $M-1$ Substitutionen $s_2, \ldots, s_M$ unterwirft, nenne ich ein **invariantes Ideal.** Ein invariantes Ideal $\mathfrak{J}$ besitzt die folgende Eigenschaft:

Hülfssatz 11. Die $M!$te Potenz eines jeden invarianten Ideals $\mathfrak{J}$ ist gleich einer ganzen rationalen Zahl.

Beweis. Es sei A eine Zahl des Ideals $\mathfrak{J}$, und $A_1, A_2, \ldots, A_M$ seien die M elementaren symmetrischen Functionen von $A = s_1 A, s_2 A, \ldots$ $\ldots, s_M A$. Den grössten gemeinsamen Teiler der M ganzen rationalen Zahlen

(18.) $$A_1^{\frac{M!}{1}},\quad A_2^{\frac{M!}{2}},\quad \ldots,\quad A_M^{\frac{M!}{M}}$$

bezeichnen wir mit A. In gleicher Weise denken wir uns zu jeder anderen Zahl $B, \Gamma, \ldots$ des Ideals $\mathfrak{J}$ und ihren conjugirten die betreffenden elementaren symmetrischen Functionen berechnet und die Teiler $\mathsf{B}, \mathsf{C}, \ldots$ in entsprechender Weise abgeleitet. Der grösste gemeinsame Teiler aller möglichen dabei auftretenden Zahlen $\mathsf{A}, \mathsf{B}, \mathsf{C}, \ldots$ werde mit J bezeichnet. Dann ist $\mathfrak{J}^{M!} = J$. In der That: da die zu A conjugirten Zahlen ebenfalls Zahlen des Ideals $\mathfrak{J}$ sind, so ist

$$A_1 \equiv 0,\ (\mathfrak{J}),\quad A_2 \equiv 0,\ (\mathfrak{J}^2),\quad \ldots,\quad A_M \equiv 0,\ (\mathfrak{J}^M);$$

und folglich sind die sämtlichen Zahlen (18.) und mithin auch $\mathsf{A} \equiv 0$ nach $\mathfrak{J}^{M!}$. Da das Gleiche auch von den Zahlen $\mathsf{B}, \mathsf{C}, \ldots$ gilt, so ist auch $J \equiv 0$ nach $\mathfrak{J}^{M!}$. Andererseits sind die Coefficienten $A_1, A_2, \ldots, A_M$ der Gleichung Mten Grades für A bezüglich durch $J^{\frac{1}{M!}}, J^{\frac{2}{M!}}, \ldots, J^{\frac{M}{M!}}$ teilbar, und somit ist A selbst durch $J^{\frac{1}{M!}}$ teilbar. Da das Nämliche

von allen Zahlen B, Γ, ... des Ideals $\mathfrak{J}$ gilt, so ist $\mathfrak{J}^{M!}$ durch J teilbar.

Aus dem eben bewiesenen Hülfssatz 11 folgt unmittelbar die weitere Thatsache:

Satz 67. Zu einem jeden beliebigen Ideal $\mathfrak{A}$ des Galois'schen Körpers K lässt sich stets ein Ideal $\mathfrak{B}$ so finden, dass das Product $\mathfrak{A}\mathfrak{B}$ ein Hauptideal wird.

Beweis. Das Ideal $\mathfrak{J} = \mathfrak{A}.s_2\mathfrak{A} \ldots s_M\mathfrak{A}$ ist offenbar ein invariantes Ideal; es ist daher nach dem Hülfssatz 11 das Ideal

$$\mathfrak{B} = \mathfrak{J}^{M!-1} s_2\mathfrak{A} \ldots s_M\mathfrak{A}$$

ein Ideal von der Art, wie es Satz 67 verlangt.

Der Satz 67 gestattet, die weiteren Teilbarkeitsgesetze für die Ideale des Galois'schen Körpers in derselben Weise zu entwickeln, wie dies in § 5 auf Grund des Satzes 8 für einen beliebigen Zahlkörper k geschehen ist.

Um dann aus den Teilbarkeitsgesetzen innerhalb des Galois'schen Körpers die Teilbarkeitsgesetze für einen beliebigen Körper k abzuleiten, beweise man entweder zunächst im Galois'schen Körper die Kronecker'schen Sätze 13 und 14 über Formen und schliesse hieraus die Richtigkeit dieser Sätze für den Unterkörper k, oder man wende ein geeignetes directes Uebergangsverfahren an. [*Hilbert*[2].]

§ 37.

Die Elemente, die Differente und die Discriminante des Galois'schen Körpers.

Im Galois'schen Körper K erhalten manche der früher eingeführten Begriffe eine einfachere Bedeutung. So sind die Elemente eines Galois'schen Körpers stets Ideale in diesem Körper selbst, und zwar gelten d[ie] Thatsachen:

Satz 68. Die Elemente eines Galois'schen Körpers K vertausch[en] sich unter einander bei Anwendung einer der M Substitutionen $s_1, \ldots, s_M$. Die Differente $\mathfrak{D}$ des Körpers K ist ein invariantes Ideal, und die Discriminante $D = \pm N(\mathfrak{D})$ ist daher, als Ideal, die Mte Potenz der Differente $\mathfrak{D}$.

Beweis. Bezeichnen wir mit $\Omega_1, \ldots, \Omega_M$ eine Basis des Körpers K, so sind die Elemente von K Ideale von der Gestalt:

$$\mathfrak{E}_2 = (\Omega_1 - s_2\Omega_1, \quad \ldots, \quad \Omega_M - s_2\Omega_M),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\mathfrak{E}_M = (\Omega_1 - s_M\Omega_1, \quad \ldots, \quad \Omega_M - s_M\Omega_M).$$

Wenden wir irgend eine der Substitutionen s auf eines dieser Elemente $\mathfrak{E}_i$ an und bedenken, dass die Zahlen $s\Omega_1, \ldots, s\Omega_M$ wiederum eine Basis des Körpers darstellen müssen, so folgt, wenn $ss_i = s_{i'}s$ gesetzt wird:

$$s\mathfrak{E}_i = (s\Omega_1 - s_{i'}s\Omega_1, \quad \ldots, \quad s\Omega_M - s_{i'}s\Omega_M) = \mathfrak{E}_{i'}.$$

Die Invarianz der Körperdifferente folgt nunmehr aus ihrer Darstellung $\mathfrak{D} = \mathfrak{E}_2 \ldots \mathfrak{E}_M$.

§ 38.

Die Unterkörper des Galois'schen Körpers.

Der Galois'sche Körper gestattet ein sehr genaues Studium der Zerlegungsgesetze seiner Zahlen mit Rücksicht auf die in ihm enthaltenen Unterkörper, und die hierbei sich ergebenden Resultate sind vor allem für die Anwendung der allgemeinen Körpertheorie auf besondere Zahlkörper von Wichtigkeit. [*Hilbert*[3].]

Um einen beliebigen Unterkörper des Galois'schen Körpers in einfacher Art zu charakterisiren, bedienen wir uns folgender Ausdrucksweise. Wenn r Substitutionen $s_1 = 1, s_2, \ldots, s_r$ der Gruppe G eine Untergruppe g vom $r$ten Grade liefern, so bildet offenbar die Gesamtheit aller derjenigen Zahlen des Körpers K, welche bei Anwendung einer jeden Substitution von g ungeändert bleiben, einen in K enthaltenen Körper k vom Grade $m = \frac{M}{r}$. Dieser Körper k heisse der **zur Untergruppe g gehörige Unterkörper.** Der Galois'sche Körper selbst gehört zu der Gruppe, welche allein aus $s_1 = 1$ besteht; zur Gruppe G aller M Substitutionen s gehört der Körper der rationalen Zahlen. Umgekehrt gehört ein jeder Unterkörper k des Galois'schen Körpers zu einer gewissen Untergruppe g der Gruppe G. Diese Gruppe g heisse die **den Unterkörper k bestimmende Untergruppe.**

§ 39.

Der Zerlegungskörper und der Trägheitskörper eines Primideals $\mathfrak{P}$.

Wählen wir nun ein bestimmtes Primideal $\mathfrak{P}$ vom Grade f im Galois'schen Körper K aus, so giebt es eine ganz bestimmte Reihe in einander geschachtelter Unterkörper von K, welche für das Primideal $\mathfrak{P}$ charakteristisch sind, und deren merkwürdige Eigenschaften jetzt kurz entwickelt werden sollen.

Es sei p die durch $\mathfrak{P}$ teilbare rationale Primzahl; ferner seien $z, z', z'', \ldots$ diejenigen sämtlichen r_z Substitutionen der Gruppe G, welche das Primideal $\mathfrak{P}$ ungeändert lassen; dieselben bilden eine Gruppe vom $r_z$ten Grade, welche die **Zerlegungsgruppe des Primideals** $\mathfrak{P}$ genannt und mit g_z bezeichnet werden soll. Der zur Zerlegungsgruppe g_z gehörige Körper k_z werde **Zerlegungskörper des Primideals** $\mathfrak{P}$ genannt; derselbe ist vom Grade $m_z = \frac{M}{r_z}$.

Weiter seien $t, t', t'', \ldots$ sämtliche unter den Substitutionen s der Gruppe G von der Beschaffenheit, dass für jede beliebige ganze Zahl Ω des Körpers K die Congruenz $s\Omega \equiv \Omega$ nach $\mathfrak{P}$ erfüllt ist und r_t deren Anzahl; es folgt leicht, dass diese r_t Substitutionen eine Gruppe $r_t$ten Grades bilden. Diese Gruppe werde die **Trägheitsgruppe des Primideals** $\mathfrak{P}$ genannt und mit g_t bezeichnet. Der zur Trägheitsgruppe g_t gehörige Körper k_t werde **Trägheitskörper des Primideals** $\mathfrak{P}$ genannt; derselbe ist vom Grade $m_t = \frac{M}{r_t}$.

Das Verhältnis der Trägheitsgruppe zur Zerlegungsgruppe wird durch folgende Thatsachen klargestellt:

Satz 69. Die Trägheitsgruppe g_t des Primideals $\mathfrak{P}$ ist eine invariante Untergruppe der Zerlegungsgruppe g_z. Man erhält alle Substitutionen der Zerlegungsgruppe und jede nur einmal, wenn man die Substitutionen der Trägheitsgruppe mit $1, z, z^2, \ldots, z^{f-1}$ multiplicirt, wo z eine geeignet gewählte Substitution der Zerlegungsgruppe ist.

Beweis. Es sei t eine beliebige Substitution in g_t und Ω eine durch $\mathfrak{P}$ teilbare ganze Zahl des Körpers K. Setzen wir $\Omega' = t^{-1}\Omega$, so ist infolge der Eigenschaft der Trägheitsgruppe $\Omega' \equiv t\Omega' \equiv \Omega$ nach $\mathfrak{P}$, d. h. $\Omega' \equiv 0$ nach $\mathfrak{P}$. Die Anwendung der Substitution t ergiebt $\Omega \equiv 0$ nach dem Primideal $t\mathfrak{P}$. Da diese Congruenz für jede Zahl Ω des Primideals $\mathfrak{P}$ gilt, so muss $\mathfrak{P}$ durch $t\mathfrak{P}$ teilbar sein, und folglich ist $\mathfrak{P} = t\mathfrak{P}$, d. h. die Trägheitsgruppe g_t ist eine Untergruppe der Zerlegungsgruppe g_z.

Um die übrigen Behauptungen des Satzes 69 zu beweisen, bestimmen wir eine Primitivzahl $\boldsymbol{P}$ des Primideals $\mathfrak{P}$, welche congruent 0 nach allen zu $\mathfrak{P}$ conjugirten und von $\mathfrak{P}$ verschiedenen Primidealen ist. Die Möglichkeit der Bestimmung einer solchen Primitivzahl folgt aus Satz 25; dann bilden wir die ganzzahlige Function Mten Grades von x

$$F(x) = (x - s_1\boldsymbol{P})(x - s_2\boldsymbol{P})\ldots(x - s_M\boldsymbol{P}).$$

Da $\boldsymbol{P}$ eine Wurzel der ganzzahligen Congruenz $F(x) \equiv 0$ nach $\mathfrak{P}$ ist, so genügt nach Satz 27 auch $\boldsymbol{P}^p$ der nämlichen Congruenz, und hieraus folgt, dass es unter den M Substitutionen $s_1, \ldots, s_M$ notwendig eine Substitution s von der Art giebt, dass $s\boldsymbol{P} \equiv \boldsymbol{P}^p$ nach $\mathfrak{P}$ wird. Wäre nun $s^{-1}\mathfrak{P} \neq \mathfrak{P}$, so bestände infolge der Wahl von $\boldsymbol{P}$ die Congruenz $\boldsymbol{P} \equiv 0$ nach $s^{-1}\mathfrak{P}$, und folglich müsste $s\boldsymbol{P} \equiv 0$ nach $\mathfrak{P}$ sein, was der vorhin gefundenen Congruenz widerspräche.

Wegen $s\mathfrak{P} = \mathfrak{P}$ gehört die Substitution s zur Zerlegungsgruppe. Wir setzen $s = z$. Die wiederholte Anwendung der Substitution z auf die Congruenz $z\boldsymbol{P} \equiv \boldsymbol{P}^p$ nach $\mathfrak{P}$ liefert die weiteren Congruenzen $z^2\boldsymbol{P} \equiv \boldsymbol{P}^{p^2}$, $z^3\boldsymbol{P} \equiv \boldsymbol{P}^{p^3}, \ldots, z^f\boldsymbol{P} \equiv \boldsymbol{P}^{p^f} \equiv \boldsymbol{P}$ nach $\mathfrak{P}$. Infolge der letzten Congruenz ist z^f eine Substitution der Trägheitsgruppe. Denn jede beliebige ganze Zahl Ω des Körpers K kann in der Gestalt $\Omega = \boldsymbol{P}^a + \boldsymbol{\Pi}$ oder $= \boldsymbol{\Pi}$ dargestellt werden, wo a eine ganze rationale Zahl und $\boldsymbol{\Pi}$ eine durch $\mathfrak{P}$ teilbare Zahl des Körpers bedeutet. Wegen $z^f\mathfrak{P} = \mathfrak{P}$ folgt daraus in der That $z^f\Omega \equiv \Omega$ nach $\mathfrak{P}$.

Die Congruenz $z\boldsymbol{P} \equiv \boldsymbol{P}^p$ nach $\mathfrak{P}$ lehrt, dass $z^{-1}tz\boldsymbol{P} \equiv \boldsymbol{P}$ nach $\mathfrak{P}$ ist, wo t eine beliebige Substitution der Trägheitsgruppe g_t bedeutet. Setzen wir $z' = z^{-1}tz$ und verstehen unter Ω eine beliebige ganze Zahl des Körpers K, so folgt wenn Ω der Congruenz $\Omega \equiv \boldsymbol{P}^a$ nach $\mathfrak{P}$ genügt, $z\Omega \equiv (z\boldsymbol{P})^a \equiv \boldsymbol{P}^a \equiv \Omega$ nach $\mathfrak{P}$, und desgleichen, wenn $\Omega \equiv 0$ nach $\mathfrak{P}$ ist, d. h. $z' = z^{-1}tz$ gehört der Trägheitsgruppe an.

Es sei nun $P(\boldsymbol{P})$ diejenige ganzzahlige Function $f$ten Grades von $\boldsymbol{P}$, welche $\equiv 0$ nach $\mathfrak{P}$ ist; nach Satz 27 hat die Congruenz $P(x) \equiv 0$ nach $\mathfrak{P}$ die Wurzeln $\boldsymbol{P}, \boldsymbol{P}^p, \ldots, \boldsymbol{P}^{p^{f-1}}$, und nach Satz 26 besitzt sie keine anderen Congruenzwurzeln.

Ist nun z^* eine beliebige Substitution der Zerlegungsgruppe, so folgt aus der Congruenz $P(\boldsymbol{P}) \equiv 0$ nach $\mathfrak{P}$ notwendig $P(z^*\boldsymbol{P}) \equiv 0$, und daher muss $z^*\boldsymbol{P} \equiv \boldsymbol{P}^{p^i}$ nach $\mathfrak{P}$ sein, wo i einen der f Werte $0, 1, \ldots, f-1$ hat. Da andererseits $\boldsymbol{P}^{p^i} \equiv z^i\boldsymbol{P}$ ist, so wird $z^{-i}z^*\boldsymbol{P} \equiv \boldsymbol{P}$ nach $\mathfrak{P}$, und mithin ist $z^{-i}z^*$ eine Substitution t der Trägheitsgruppe, d. h. $z^* = z^i t$. In dieser letzteren Gestalt sind also sämtliche Substitutionen $z, z', z'', \ldots$ der Zerlegungsgruppe darstellbar, und da auch umgekehrt $z^i t$ für $i = 0, 1, \ldots, f-1$ lauter von einander verschiedene Substitutionen darstellt, so ist der letzte Teil des Satzes 69 bewiesen. Endlich erhellt jetzt auch die Invarianz der Trägheitsgruppe aus der oben bewiesenen Thatsache, dass $z^{-1}tz$ stets zu dieser Gruppe gehört.

Zugleich ergiebt sich $r_z = fr_t$.

§ 40.

Ein Satz über den Zerlegungskörper.

Die wichtigste Eigenschaft des Zerlegungskörpers findet in folgendem Satze ihren Ausdruck:

Satz 70. Das Ideal $\mathfrak{p}=\mathfrak{P}^{r_t}$ liegt im Zerlegungskörper k_z und ist in diesem ein Primideal ersten Grades. Im Zerlegungskörper k_z wird $p=\mathfrak{p}\mathfrak{a}$, wo $\mathfrak{a}$ ein zu $\mathfrak{p}$ primes Ideal ist.

Beweis. Die Relativnorm des Primideals $\mathfrak{P}$ in Bezug auf den Körper k_z ist $N_{k_z}(\mathfrak{P})=\mathfrak{P}^{r_z}$. Um nun die niedrigste in k_z liegende Potenz des Primideals $\mathfrak{P}$ zu ermitteln, denken wir uns den grössten gemeinsamen Teiler aller derjenigen ganzen Zahlen des Körpers k_z bestimmt, welche durch $\mathfrak{P}$ teilbar sind. Dieser Teiler ist notwendig im Körper k_z ein Primideal $\mathfrak{p}$, und, da $\mathfrak{P}^{r_z}$ in k_z liegt, so ist $\mathfrak{p}$ jedenfalls eine Potenz von $\mathfrak{P}$; wir setzen $\mathfrak{p}=\mathfrak{P}^u$. Zur Bestimmung des Exponenten u dient die folgende Betrachtung. Soll eine durch $\mathfrak{P}$ nicht teilbare Zahl A des Körpers K der Congruenz $A\equiv zA$ nach $\mathfrak{P}$ genügen, und ist etwa $A\equiv \boldsymbol{P}^i$ nach $\mathfrak{P}$, so muss notwendig $i\equiv pi$ nach p^f-1 und folglich i eine durch $1+p+p^2+\cdots+p^{f-1}$ teilbare Zahl sein, d. h. es giebt nur $p-1$ einander nach $\mathfrak{P}$ incongruente Zahlen von der gewünschten Beschaffenheit, und es wird daher $A\equiv a$ nach $\mathfrak{P}$, wo a eine ganze rationale Zahl bedeutet. Aus dieser Betrachtung folgt insbesondere, dass jede Zahl α des Körpers k_z einer rationalen Zahl a nach $\mathfrak{P}$ und mithin auch nach $\mathfrak{p}$ congruent ist, d. h. $\mathfrak{p}$ ist im Körper k_z ein Primideal ersten Grades, und die Norm $n(\mathfrak{p})$ im Körper k_z ist folglich gleich p. Andererseits ist die Norm von $\mathfrak{p}$ im Körper K durch die Formel $N(\mathfrak{p})=[n(\mathfrak{p})]^{r_z}$ gegeben, und wegen $\mathfrak{p}=\mathfrak{P}^u$ und $N(\mathfrak{P})=p^f$ folgt somit $p^{uf}=p^{r_z}$, d. h. $u=r_t$.

Aus der Definition der Zerlegungsgruppe ergiebt sich $N(\mathfrak{P})=\mathfrak{P}^{r_z}\mathfrak{A}$, wo $\mathfrak{A}$ ein zu $\mathfrak{P}$ primes Ideal bedeutet. Setzen wir $p=\mathfrak{p}\mathfrak{a}$, so wird $N(\mathfrak{P})=p^f=\mathfrak{p}^f\mathfrak{a}^f$ und folglich $\mathfrak{a}^f=\mathfrak{A}$, womit auch der letzte Teil des Satzes 70 bewiesen ist.

§ 41.

Der Verzweigungskörper eines Primideals $\mathfrak{P}$.

Um den Bau der Trägheitsgruppe näher zu erforschen, bezeichnen wir jetzt mit A eine feste durch $\mathfrak{P}$, aber nicht durch $\mathfrak{P}^2$ teilbare Zahl des Körpers K und ermitteln für alle Substitutionen $t, t', t'', \ldots$ der Trägheitsgruppe die Congruenzen

$$\left.\begin{array}{l} t\ A \equiv P^a\ A \\ t'\ A \equiv P^{a'}\ A \\ t''\ A \equiv P^{a''}\ A \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \end{array}\right\}, \quad (\mathfrak{P}^2),$$

wo $a, a', a'', \ldots$ Zahlen aus der Reihe $0, 1, 2, \ldots, p^f-2$ bedeuten. Diejenigen unter den Substitutionen $t, t', t'', \ldots$, für welche die betreffenden Exponenten $a, a', a'', \ldots$ den Wert 0 haben, mögen mit $v, v', v'', \ldots$ bezeichnet werden; ihre Anzahl sei r_v; sie bilden, wie leicht ersichtlich, eine invariante Untergruppe der Trägheitsgruppe. Diese Untergruppe $r_v$ten Grades werde die **Verzweigungsgruppe des Primideals** $\mathfrak{P}$ genannt und mit g_v bezeichnet. Der zu g_v gehörige Körper k_v heisse der **Verzweigungskörper des Primideals** $\mathfrak{P}$. Das Verhältniss der Verzweigungsgruppe zur Trägheitsgruppe wird genauer durch folgenden Satz charakterisirt:

Satz 71. Die Verzweigungsgruppe g_v ist eine invariante Untergruppe der Trägheitsgruppe; der Grad r_v derselben ist eine Potenz von p, etwa $r_v = p^l$. Man erhält alle Substitutionen der Trägheitsgruppe und jede nur einmal, indem man die Substitutionen der Verzweigungsgruppe mit $1, t, t^2, \ldots, t^{h-1}$ multiplicirt, wo $h = \frac{r_t}{r_v}$ und t eine geeignet gewählte Substitution der Trägheitsgruppe ist. Die Zahl h ist ein Teiler von p^f-1.

Beweis. Es sei $\mathfrak{P}^u$ eine so hohe Potenz von $\mathfrak{P}$, dass für jede von 1 verschiedene Substitution v der Verzweigungsgruppe die Incongruenz $vA \not\equiv A$ nach $\mathfrak{P}^u$ gilt. Setzen wir nun $vA \equiv A + BA^2$ nach $\mathfrak{P}^3$, wo B eine ganze Zahl in K bedeutet, so folgt leicht $v^p A \equiv A$ nach $\mathfrak{P}^3$ und hieraus in entsprechender Weise $v^{p^2} A \equiv A$ nach $\mathfrak{P}^4$ u. s. w., endlich $v^{p^{u-2}} A \equiv A$ nach $\mathfrak{P}^u$. Demnach ist $v^{p^{u-2}} = 1$, d. h. der Grad r_v der Verzweigungsgruppe ist gleich einer Potenz von p; wir setzen $r_v = p^l$.

Es sei nun a der kleinste von 0 verschiedene unter den Exponenten $a, a', a'', \ldots$, und es gebe im ganzen h verschiedene Zahlen unter diesen Exponenten. Dann sind diese Zahlen notwendig Vielfache von a und stimmen mit den Zahlen $0, a, 2a, \ldots, (h-1)a$ überein; es ist ferner $ha = p^f - 1$. Zugleich erkennen wir, dass alle Substitutionen der Trägheitsgruppe in die Gestalt $t^i v$ gebracht werden können, wo i die Werthe $0, 1, \ldots, h-1$ annimmt und v alle Substitutionen der Verzweigungsgruppe g_v durchläuft. Es ist folglich $r_t = h r_v$.

§ 42.
Ein Satz über den Trägheitskörper.

Ueber das Verhalten der Ideale $\mathfrak{P}$ und $\mathfrak{p}$ im Körper k_t giebt der folgende Satz Aufschluss:

Satz 72. Jede Zahl des Körpers K ist nach $\mathfrak{P}$ einer Zahl des Trägheitskörpers congruent. Der Trägheitskörper bewirkt keine Zerlegung des Ideals $\mathfrak{p}$, sondern nur eine Graderhöhung desselben, insofern $\mathfrak{p}$ beim Uebergang vom Körper k_z in den oberen Körper k_t aus einem Primideal ersten Grades sich in ein Primideal $f$ten Grades verwandelt.

Beweis. Wir setzen

$$\pi = \{v\boldsymbol{P}.v'\boldsymbol{P}.v''\boldsymbol{P}\ldots\}^{p^{l(f-1)}},$$

$$\varkappa = \frac{1}{h}(\pi + t\pi + t^2\pi + \cdots + t^{h-1}\pi);$$

unter $\boldsymbol{P}$ wieder eine Primitivzahl nach $\mathfrak{P}$ und unter t die Substitution aus Satz 71 verstanden; die Zahl π liegt im Körper k_v und die Zahl $\varkappa$ im Körper k_t. Um letzteres zu beweisen, bedenke man, dass die Zahl $\varkappa$ bei Anwendung der Substitution t ungeändert bleibt, weil t^h zu g_v gehört, und dass die Zahlen π, $t\pi$, $t_2\pi$, ..., $t^{h-1}\pi$ bei Anwendung einer Substitution aus g_v ungeändert bleiben. Diese Zahlen π und $\varkappa$ sind, wie man leicht einsieht, beide nach dem Primideal $\mathfrak{P}$ der Primitivzahl $\boldsymbol{P}$ congruent. Da es folglich im Körper k_t genau p^f nach $\mathfrak{P}$ incongruente Zahlen giebt, so ist notwendigerweise $\mathfrak{p} = \mathfrak{P}^{r_t}$ im Körper k_t unzerlegbar und wird in demselben ein Primideal $f$ten Grades.

§ 43.
Sätze über die Verzweigungsgruppe und den Verzweigungskörper.

Es ist nun leicht, die charakteristische Eigenschaft der Verzweigungsgruppe zu erkennen; dieselbe ist folgende:

Satz 73. Zur Verzweigungsgruppe g_v gehören alle und nur solche Substitutionen s, bei deren Anwendung für sämtliche ganze Zahlen Ω des Körpers K die Congruenz $s\Omega \equiv \Omega$ nach $\mathfrak{P}^2$ besteht.

Beweis. Es sei die beliebige Zahl Ω in K der Zahl ω des Trägheitskörpers nach $\mathfrak{P}$ congruent, und dementsprechend werde $\Omega - \omega \equiv BA$ nach $\mathfrak{P}^2$ gesetzt, wo A die Bedeutung wie in § 41 hat und B eine geeignete ganze Zahl in K ist. Durch die Anwendung einer Substitution v des Verzweigungskörpers ergiebt sich $v\Omega - \omega \equiv v(BA) \equiv BA \equiv \Omega - \omega$, d. h. $v\Omega \equiv \Omega$ nach $\mathfrak{P}^2$.

Zugleich erkennen wir leicht den folgenden weiteren Satz über den Verzweigungskörper:

Satz 74. Das Ideal $\mathfrak{p}_v = \mathfrak{P}^{r_v}$ liegt im Verzweigungskörper und ist in demselben ein Primideal $f$ten Grades: es findet somit im Verzweigungskörper die Spaltung des Ideals $\mathfrak{p} = \mathfrak{p}_v^h$ in h gleiche Primfactoren statt.

§ 44.

Die überstrichenen Verzweigungskörper eines Primideals $\mathfrak{P}$.

Unsere nächste Aufgabe besteht darin, weiter die Spaltung des Ideals $\mathfrak{p}_v$ in gleiche Factoren zu verfolgen. Zu dem Zweck nehmen wir an, es sei L der höchste Exponent von der Art, dass für eine jede Substitution v der Verzweigungsgruppe die sämtlichen ganzen Zahlen des Körpers K der Congruenz $v\Omega \equiv \Omega$ nach $\mathfrak{P}^L$ genügen, und bestimmen dann alle Substitutionen s der Verzweigungsgruppe, für welche $s\Omega \equiv \Omega$ nach $\mathfrak{P}^{L+1}$ wird; dieselben bilden eine Untergruppe $g_{\bar v}$ der Verzweigungsgruppe, die wir die **einmal überstrichene Verzweigungsgruppe des Primideals** $\mathfrak{P}$ nennen. Der zu g_v gehörige Körper $k_{\bar v}$ heisse der **einmal überstrichene Verzweigungskörper des Primideals.** Die wichtigsten Eigenschaften dieses Körpers sind folgende:

Satz 75. Die einmal überstrichene Verzweigungsgruppe $g_{\bar v}$ ist eine invariante Untergruppe der Verzweigungsgruppe g_v. Der Grad von $g_{\bar v}$ sei $r_{\bar v} = p^{\bar l}$. Man erhält alle Substitutionen der Verzweigungsgruppe g_v und jede nur einmal, indem man die Substitutionen der einmal überstrichenen Verzweigungsgruppe $g_{\bar v}$ mit gewissen $p^{\bar e}$ Substitutionen $v_1, \ldots, v_{p^{\bar e}}$ der Verzweigungsgruppe g_v multiplicirt; dabei haben diese $p^{\bar e}$ Substitutionen die Besonderheit, dass für irgend zwei derselben v_i und $v_{i'}$ stets eine Relation von der Gestalt $v_i v_{i'} = v_{i'} v_i \bar v$ besteht, wo $\bar v$ eine Substitution in $g_{\bar v}$ ist. Das Ideal $\mathfrak{p}_{\bar v} = \mathfrak{P}^{r_{\bar v}}$ ist Primideal in $k_{\bar v}$: es findet somit in $k_{\bar v}$ die Spaltung des Ideals $\mathfrak{p}_v = \mathfrak{p}_{\bar v}^{p^{\bar e}}$ in $p^{\bar e}$ gleiche Primfactoren statt; dabei ist der Exponent $\bar e$ eine Zahl, die den Grad f des Primideals $\mathfrak{P}$ nicht überschreitet.

Beweis. Es sei A eine durch $\mathfrak{P}$, aber nicht durch $\mathfrak{P}^2$ teilbare ganze Zahl des Körpers K; wir bestimmen dann ein System von Substitutionen $v_1, \ldots, v_r$ der Verzweigungsgruppe von der Art, dass, wenn

$$v_1 A \equiv A + B_1 A^L, \quad \ldots, \quad v_r A \equiv A + B_r A^L, \quad (\mathfrak{P}^{L+1})$$

gesetzt wird, die ganzen Zahlen $B_1, \ldots, B_r$ sämtlich einander nach

$\mathfrak{P}$ incongruent sind und auch keine Substitution von g_v zu diesem Systeme $v_1, \ldots, v_r$ hinzugefügt werden kann, ohne der letzteren Forderung zu widersprechen. Wählen wir dann eine beliebige Substitution v^* der Verzweigungsgruppe g_v und setzen $v^* A \equiv A + BA^L$ nach $\mathfrak{P}^{L+1}$, so muss B einer der Zahlen $B_1, \ldots, B_r$ nach $\mathfrak{P}$ congruent sein; ist etwa $B \equiv B_i$ nach $\mathfrak{P}$, so folgt $v_i^{-1} v^* A \equiv 0$ nach $\mathfrak{P}^{L+1}$. Aus Satz 72 folgt, dass jede ganze Zahl Ω in K einem Ausdrucke $\alpha_t + \beta_t A + \cdots + \lambda_t A^L$ nach $\mathfrak{P}^{L+1}$ congruent ist, wo $\alpha_t, \beta_t, \ldots, \lambda_t$ ganze Zahlen des Trägheitskörpers sind, und hieraus ergiebt sich für Ω die Congruenz $v_i^{-1} v^* \Omega \equiv \Omega$ nach $\mathfrak{P}^{L+1}$, d. h. es ist $v_i^{-1} v^* = \bar{v}$ oder $v^* = v_i \bar{v}$. Diese Gleichung beweist die im Satze 75 behauptete Structur der Gruppe $g_{\bar v}$.

Wir setzen $r_{\bar v} = p^{\bar l}$ und $\bar e = l - \bar l$.

Es ist nunmehr ersichtlich, in welcher Weise das eingeschlagene Verfahren fortzusetzen ist. Bedeutet $\bar L$ den höchsten Exponenten von der Art, dass für jede Substitution $\bar v$ die sämtlichen Zahlen des Körpers K der Congruenz $\bar v \Omega \equiv \Omega$ nach $\mathfrak{P}^{\bar L}$ genügen, so bestimmen wir alle die Substitutionen $\bar{\bar v}$, für welche beständig $\bar{\bar v} \Omega \equiv \Omega$ nach $\mathfrak{P}^{\bar L + 1}$ wird. Dieselben bilden eine invariante Untergruppe $g_{\bar{\bar v}}$ der Gruppe $g_{\bar v}$: die **zweimal überstrichene Verzweigungsgruppe des Primideals** $\mathfrak{P}$; ihr Grad sei $r_{\bar{\bar v}} = p^{\bar{\bar l}}$; wir setzen $\bar{\bar e} = \bar l - \bar{\bar l}$. Es wird $\mathfrak{p}_{\bar v} = \mathfrak{p}_{\bar{\bar v}}^{p^{\bar{\bar e}}}$, wo $\mathfrak{p}_{\bar{\bar v}}$ ein Primideal des zu $g_{\bar{\bar v}}$ gehörigen Körpers $k_{\bar{\bar v}}$ ist.

So fortfahrend, gelangen wir zur **dreimal überstrichenen Verzweigungsgruppe** $g_{\bar{\bar{\bar v}}}$ u. s. w. Ist etwa die i-**mal überstrichene Verzweigungsgruppe des Primideals** $\mathfrak{P}$ diejenige, welche lediglich aus der Substitution 1 besteht, so ist der i-**mal überstrichene Verzweigungskörper des Primideals** $\mathfrak{P}$ der Körper K selbst und die Structur der Verzweigungsgruppe g_v ist dann genau bekannt. Es leuchtet ein, dass für das Primideal $\mathfrak{P}$ überstrichene Verzweigungskörper nur dann vorhanden sein können, wenn der Grad M des Körpers K durch p teilbar ist.

§ 45.

Kurze Zusammenfassung der Sätze über die Zerlegung einer rationalen Primzahl p im Galois'schen Körper.

Durch die in § 39—44 entwickelten Sätze erlangen wir einen vollständigen Einblick in die bei der Zerlegung einer rationalen Primzahl p in einem Galois'schen Körper sich abspielenden Vorgänge:

Es handle sich um einen bestimmten Primfactor $\mathfrak{P}$ von p, so wird p zunächst im Zerlegungskörper von $\mathfrak{P}$ in der Form $p = \mathfrak{p}\mathfrak{a}$ zerlegt, wo $\mathfrak{p}$ ein

Primideal ersten Grades und $\mathfrak{a}$ ein durch $\mathfrak{p}$ nicht teilbares Ideal des Zerlegungskörpers ist. Der Zerlegungskörper von $\mathfrak{P}$ ist als Unterkörper in dem Trägheitskörper von $\mathfrak{P}$ enthalten, welcher seinerseits keine weitere Zerlegung von $\mathfrak{p}$ bewirkt, sondern lediglich dieses Ideal $\mathfrak{p}$ zu einem Primideal $f$ten Grades erweitert. Ist der Körper K selbst der Zerlegungskörper oder der Trägheitskörper, so ist nach diesem ersten Schritte die Zerlegung bereits abgeschlossen. Im anderen Falle lässt sich $\mathfrak{p}$ für K noch in gleiche Factoren spalten, und zwar wird $\mathfrak{p}$ zunächst im Verzweigungskörper die Potenz eines Primideals $\mathfrak{p}_v$, wobei der Exponent in $p^f - 1$ aufgeht und folglich nicht durch p teilbar ist. Die Spaltung von $\mathfrak{p}$ ist mit diesem zweiten Schritte notwendig dann und nur dann abgeschlossen, wenn p im Grade der Trägheitsgruppe nicht aufgeht und mithin der Körper K selbst der Verzweigungskörper ist. In den nun folgenden überstrichenen Verzweigungskörpern schreitet die Spaltung ohne Aussetzen fort, und zwar sind die bezüglichen Potenzexponenten Zahlen von der Gestalt $p^{\bar{e}}$, $p^{\bar{\bar{e}}}$, ..., wo keiner der Exponenten $\bar{e}$, $\bar{\bar{e}}$, ... den Grad f des Primideals $\mathfrak{P}$ überschreitet.

Die Uebersicht über die entwickelten Resultate wird durch die folgende Tabelle erleichtert, in deren Zeilen der Reihe nach die betreffenden Körper die Grade der zugehörigen Gruppen, die Grade der Körper, ihre Relativgrade in Bezug auf den nächst niederen Körper, dann die Primideale der Körper und ihre Darstellung als Potenzen von $\mathfrak{P}$ sich angegeben finden. Der Körper K ist dabei als ein dreimal überstrichener Verzweigungskörper angenommen.

k_z	k_t	k_v	$k_{\bar{v}}$	$k_{\bar{\bar{v}}}$	K
r_z	r_t	r_v	$r_{\bar{v}}$	$r_{\bar{\bar{v}}}$	1
$m_z = \frac{M}{r_z}$	$m_t = \frac{M}{r_t}$	$m_v = \frac{M}{r_v}$	$m_{\bar{v}} = \frac{M}{r_{\bar{v}}}$	$m_{\bar{\bar{v}}} = \frac{M}{r_{\bar{\bar{v}}}}$	M
	$f = \frac{r_z}{r_t}$	$h = \frac{r_t}{r_v}$	$p^{\bar{e}} = \frac{r_v}{r_{\bar{v}}}$	$p^{\bar{\bar{e}}} = \frac{r_{\bar{v}}}{r_{\bar{\bar{v}}}}$	$p^{\bar{\bar{\bar{e}}}} = r_{\bar{\bar{v}}}$
$\mathfrak{p} = \mathfrak{p}_v^h = \mathfrak{P}^{r_t}$		$\mathfrak{p}_v = \mathfrak{p}_{\bar{v}}^{p^{\bar{e}}} = \mathfrak{P}^{r_v}$	$\mathfrak{p}_{\bar{v}} = \mathfrak{p}_{\bar{\bar{v}}}^{p^{\bar{\bar{e}}}} = \mathfrak{P}^{r_{\bar{v}}}$	$\mathfrak{p}_{\bar{\bar{v}}} = \mathfrak{P}^{p^{\bar{\bar{\bar{e}}}}} = \mathfrak{P}^{r_{\bar{\bar{v}}}}$	$\mathfrak{P}$

Capitel XI.

Die Differenten und Discriminanten des Galois'schen Körpers und seiner Unterkörper.

§ 46.

Die Differenten des Trägheitskörpers und der Verzweigungskörper.

Eine reiche Quelle neuer Wahrheiten entspringt, wenn wir die soeben gewonnenen Resultate mit denjenigen des Capitels V in Zusammenhang bringen. So folgt unter Benutzung des Satzes 41 leicht ein Satz, welcher die wichtigste Eigenschaft des Trägheitskörpers aussagt; derselbe lautet:

Satz 76. Die Differente des zum Primideal $\mathfrak{P}$ gehörigen Trägheitskörpers ist nicht durch $\mathfrak{P}$ teilbar. Der Trägheitskörper umfasst sämtliche in K enthaltenen Unterkörper, deren Differenten nicht durch $\mathfrak{P}$ teilbar sind.

Betreffs der Differenten der Verzweigungskörper gelten folgende Sätze:

Satz 77. Die Relativdifferente des Verzweigungskörpers in Bezug auf den Trägheitskörper ist durch $\mathfrak{P}^{r_t - r_v} = \mathfrak{p}_v^{h-1}$ und durch keine höhere Potenz von $\mathfrak{P}$ teilbar.

Beweis. Wir bezeichnen mit α eine durch $\mathfrak{p}_v = \mathfrak{P}^{r_v}$, aber nicht durch $\mathfrak{p}_v^2$ teilbare ganze Zahl in k_v und mit A eine durch $\mathfrak{P}$, aber nicht durch $\mathfrak{P}^2$ teilbare ganze Zahl in K. Setzen wir dann $\dfrac{\alpha}{A^{r_v}} \equiv P^c$ nach $\mathfrak{P}$, wo P eine Primitivzahl nach $\mathfrak{P}$ bedeutet, so wird $\alpha \equiv P^c A^{r_v}$ nach $\mathfrak{p}_v \mathfrak{P}$. Nunmehr sei t^* eine beliebige, nicht zu g_v gehörige Substitution der Trägheitsgruppe, und es werde $t^* A \equiv P^{a^*} A$ nach $\mathfrak{P}^2$, wo a^* eine der Zahlen $a, 2a, \ldots, (h-1)a$ (vgl. § 41) bedeutet. Dann folgt

$$t^* \alpha \equiv P^{c + a^* r_v} A^{r_v} \equiv P^{a^* r_v} \alpha, \quad (\mathfrak{p}_v \mathfrak{P}).$$

Da r_v eine Potenz von p ist, so wird $P^{a^* r_v} \not\equiv 1$ nach $\mathfrak{P}$, und folglich kann $\alpha - t^* \alpha$ nicht durch $\mathfrak{p}_v \mathfrak{P}$ teilbar sein und ist mithin genau durch $\mathfrak{p}_v = \mathfrak{P}^{r_v}$ teilbar. Bedeutet ferner ω eine beliebige Zahl in k_v, so ist dieselbe nach Satz 72 notwendig einer Zahl ω_t des Trägheitskörpers nach $\mathfrak{P}$ congruent, und hieraus folgt $\omega - t^* \omega \equiv 0$ nach $\mathfrak{p}_v$. Auf diese Weise ergiebt sich, dass die in Rede stehende Relativdifferente genau durch $\mathfrak{P}^{(h-1) r_v} = \mathfrak{P}^{r_t - r_v}$ teilbar ist.

In ähnlicher Weise folgt die Thatsache:

Satz 78. Die Relativdifferente des einmal überstrichenen Verzweigungskörpers k in Bezug auf den Verzweigungskörper k_v enthält genau die Potenz $\mathfrak{P}^{L(r_v - r_{\bar v})} = \mathfrak{p}_{\bar v}^{L(p^{\bar e}-1)}$. Die Relativdifferente des zweimal überstrichenen Verzweigungskörpers $k_{\bar{\bar v}}$ in Bezug auf $k_{\bar v}$ enthält genau die Potenz $\mathfrak{P}^{\bar L(r_{\bar v} - r_{\bar{\bar v}})} = \mathfrak{p}_{\bar{\bar v}}^{\bar L(p^{\bar{\bar e}}-1)}$ u. s. w.

§ 47.

Die Teiler der Discriminante des Galois'schen Körpers.

Satz 79. Der Exponent der Potenz, zu welcher die rationale Primzahl p in der Discriminante D des Körpers K als Factor vorkommt, ist

$$m_t\{r_t - r_v + L(r_v - r_{\bar v}) + \bar L(r_{\bar v} - r_{\bar{\bar v}}) + \cdots\}.$$

Beweis. Der Satz 41 lehrt in Verbindung mit den oben ausgesprochenen Sätzen 76, 77 und 78, dass die Differente $\mathfrak{D}$ des Körpers K das Primideal $\mathfrak{P}$ genau in der $r_t - r_v + L(r_v - r_{\bar v}) + \bar L(r_{\bar v} - r_{\bar{\bar v}}) + \cdots$ ten Potenz enthält. Hieraus folgt nach Satz 68 die Richtigkeit der Behauptung.

Im Falle, dass keine überstrichenen Verzweigungskörper vorhanden sind, kommt bereits das Glied mit L nicht mehr in Frage, und es folgt dann, dass der Exponent der in D aufgehenden Potenz von p den Werth $m_t(r_t - 1)$ besitzt. Nach dem Obigen tritt dieser Fall sicher dann ein, wenn der Grad M zu p prim ist. Man vergleiche die Bemerkungen am Schluss des § 12.

Satz 80. Der Exponent der in der Discriminante D aufgehenden Potenz von der rationalen Primzahl p überschreitet nicht eine gewisse Grenze, die nur vom Grade M des Galois'schen Körpers K abhängt.

Beweis. Alle Exponenten $\bar L$, L, ... für ein Primideal $\mathfrak{P}$ liegen unter einer durch M allein bestimmten Grenze. Um für L eine solche Grenze aufzufinden, bezeichnen wir mit ω eine durch $\mathfrak{p}_{\bar v}$, aber nicht durch $\mathfrak{p}_{\bar v}^2$ teilbare ganze Zahl in $k_{\bar v}$ und wählen ein System von $p^{\bar e}$ Substitutionen $v_1, v_2, \ldots, v_{p^{\bar e}}$ der Verzweigungsgruppe aus, welche durch Zusammensetzung mit $g_{\bar v}$ diese Gruppe g_v erzeugen. Die Zahl $\alpha = v_1\omega + v_2\omega + \cdots + v_{p^{\bar e}}\omega$ bleibt dann bei allen Substitutionen g_v ungeändert und gehört daher dem Körper k_v an. Andererseits ist $\omega \equiv v\omega$ nach $\mathfrak{P}^L$ und folglich $\alpha \equiv p^{\bar e}\omega$ nach $\mathfrak{P}^L$. Wäre nun $L > \bar e r_t + r_{\bar v}$, so

müsste $\alpha \equiv 0$ nach $\mathfrak{p}^{\bar{e}}\mathfrak{p}_v$, aber $\not\equiv 0$ nach $\mathfrak{p}^{\bar{e}}\mathfrak{p}_{\bar{v}}\mathfrak{P}$ sein. Setzen wir daher $p = \mathfrak{p}\mathfrak{a}$, wo $\mathfrak{a}$ ein zu $\mathfrak{p}$ primes Ideal des Zerlegungskörpers bedeutet, und bezeichnen mit γ eine durch $\mathfrak{a}$ teilbare und zu $\mathfrak{p}$ prime Zahl des Zerlegungskörpers, so ist $\beta = \frac{\alpha\gamma^{\bar{e}}}{p^{\bar{e}}}$ eine ganze Zahl in k_v; dieselbe wäre durch $\mathfrak{p}_{\bar{v}}$, aber nicht durch $\mathfrak{p}_{\bar{v}}\mathfrak{P}$ teilbar, und mithin wäre $\mathfrak{p}_{\bar{v}}$ im Widerspruch mit Satz 75 ein Ideal des Körpers k_v. Da man in ähnlicher Weise auch für die übrigen Exponenten $\bar{L}, \ldots$ eine obere Grenze findet, so kann hiernach auch der in Satz 79 angegebene Exponent der in der Discriminante D aufgehenden Potenz von p eine gewisse, nur vom Grade M des Körpers K abhängige Grenze nicht überschreiten.

Der Satz 80 ist besonders deshalb von Wichtigkeit, weil er die Möglichkeiten, die sich hinsichtlich der in M aufgehenden Primzahlen p bieten, von vornherein auf eine endliche Anzahl einschränkt. Rechnen wir alle diejenigen Körper vom Grade M, bei welchen die Zerlegung der in M aufgehenden Primzahlen für alle obigen Anzahlen die nämlichen Werte liefert, zu einem Typus, so folgt, dass es für einen gegebenen Grad M nur eine endliche Anzahl von möglichen Körpertypen giebt.

Als Beispiel für den Satz 80 diene der (im dritten Teil ausführlich behandelte) quadratische Körper, in dessen Discriminante die ungeraden Primzahlen höchstens einfach und die Primzahl 2 höchstens zur dritten Potenz aufgeht (vgl. § 59 Satz 95).

Capitel XII.

Die Beziehungen der arithmetischen zu algebraischen Eigenschaften des Galois'schen Körpers.

§ 48.

Der relativ-Galois'sche, der relativ-Abel'sche und der relativ-cyklische Körper.

Ist die Gruppe G der Substitutionen $s_1, \ldots, s_M$ eines Galois'schen Körpers K eine Abel'sche Gruppe, d. h. sind die Substitutionen $s_1, \ldots, s_M$ unter einander vertauschbar, so heisst der Galois'sche Körper K ein **Abel'scher Körper.** Ist jene Substitutionsgruppe G insbesondere eine

cyklische, d. h. sind die M Substitutionen $s_1, \ldots, s_M$ sämtlich als Potenzen einer einzigen unter ihnen darstellbar, so heisst der Abel'sche Körper K ein **cyklischer Körper.**

Wenn wir die nämliche Betrachtung, welche in § 28 für die Idealklassen angestellt worden ist, auf die Substitutionen der Gruppe eines Abel'schen Körpers anwenden, so ergiebt sich der Satz, dass jeder Abel'sche Körper aus cyklischen Körpern zusammengesetzt werden kann. Die cyklischen Körper ihrerseits lassen sich ferner stets aus solchen besonderen cyklischen Körpern zusammensetzen, deren Grade Primzahlen oder Primzahlpotenzen sind.

Die in Rede stehenden Begriffe lassen folgende Verallgemeinerung zu:

Es sei Θ die Wurzel einer Gleichung $l$ten Grades:

$$\Theta^l + \alpha_1 \Theta^{l-1} + \cdots + \alpha_l = 0,$$

deren Coefficienten $\alpha_1, \ldots, \alpha_l$ Zahlen eines Körpers k vom $m$ten Grade sind. Diese Gleichung $l$ten Grades sei überdies im Rationalitätsbereiche k irreducibel und von der besonderen Eigenschaft, dass alle übrigen $l-1$ Wurzeln $\Theta', \ldots, \Theta^{(l-1)}$ derselben sich als ganze rationale Functionen der Wurzel Θ darstellen lassen, wobei die Coefficienten dieser Functionen Zahlen des Körpers k sind. Unter dieser Voraussetzung heisst der aus Θ und den Zahlen von k gebildete Zahlkörper K vom $M = lm$ten Grade ein **relativ-Galois'scher Körper in Bezug auf** k. Der Grad l jener Gleichung ist der Relativgrad von K. Wird etwa

$$\Theta = S_1\Theta, \quad \Theta' = S_2\Theta, \quad \ldots, \quad \Theta^{(l-1)} = S_l\Theta$$

gesetzt, so heisst die Gruppe der Substitutionen $S_1, \ldots, S_l$ die **Relativgruppe;** ist diese Gruppe eine Abel'sche, so heisst der Körper K ein **relativ-Abel'scher Körper in Bezug auf** k. Ist die Relativgruppe cyklisch, so heisst der Körper K **relativ-cyklisch** in Bezug auf k.

§ 49.

Die algebraischen Eigenschaften des Trägheitskörpers und der Verzweigungskörper. Die Darstellung der Zahlen des Galois'schen Körpers durch Wurzeln im Bereiche des Zerlegungskörpers.

Mit Benutzung der eben definirten Begriffe lassen sich in sehr einfacher Weise einige wichtige algebraische Eigenschaften des Zerlegungs- und des Trägheitskörpers, sowie der Verzweigungskörper aussprechen, welche

eine unmittelbare Folge der oben bewiesenen Eigenschaften ihrer Gruppen sind. Es ergeben sich folgende Thatsachen:

Satz 81. Der Trägheitskörper k_t ist relativ cyklisch vom Relativgrade f in Bezug auf den Zerlegungskörper k_z. Der Verzweigungskörper k_v ist relativ cyklisch vom Relativgrade h in Bezug auf den Trägheitskörper k_t. Der einmal überstrichene Verzweigungskörper $k_{\bar{v}}$ ist ein relativ Abel'scher vom Relativgrade $p^{\bar{e}}$ in Bezug auf den Verzweigungskörper k_v; der Körper $k_{\bar{\bar{v}}}$ ist ein relativ Abel'scher vom Relativgrade $p^{\bar{\bar{e}}}$ in Bezug auf $k_{\bar{v}}$ u. s. f. Die Abel'schen Relativgruppen der Körper $k_{\bar{v}}$, $k_{\bar{\bar{v}}}$, ... enthalten lediglich Substitutionen vom $p$ten Grade.

Nach diesem Satze 81 geschieht also die Spaltung in gleiche Factoren stets mittelst einer Kette Abel'scher Gleichungen, und dieses Resultat drückt eine neue überraschende Eigenschaft des Zerlegungskörpers aus:

Satz 82. *Der Zerlegungskörper eines jeden Primideals in K bestimmt einen Rationalitätsbereich, in welchem die Zahlen des ursprünglichen Galois'schen Körpers K lediglich durch Wurzelausdrücke darstellbar sind.*

Dieser Satz 82 rückt zugleich die Bedeutung der Theorie der durch Wurzelziehen lösbaren Gleichungen in helles Licht; denn er zeigt, dass bei dem Process der Zerlegung der Zahlen in Primideale die wichtigsten und schwierigsten Vorgänge sich gerade in solchen Relativkörpern abspielen, deren Zahlen in einem gewissen Rationalitätsbereiche durch Wurzelausdrücke darstellbar sind.

§ 50.

Die Dichtigkeit der Primideale ersten Grades und der Zusammenhang dieser Dichtigkeit mit den algebraischen Eigenschaften eines Zahlkörpers.

Es ist eine merkwürdige Thatsache, dass die Häufigkeit gewisser Primideale ersten Grades in einem Zahlkörper Schlüsse auf die algebraische Natur desselben zulässt. [*Kronecker*[14].]

Es sei k ein beliebiger Zahlkörper $m$ten Grades, und es bedeute allgemein p_i eine rationale Primzahl, in der genau i von einander verschiedene Primideale ersten Grades aufgehen. Wenn dann der Limes

$$\underset{s=1}{L}\left\{\frac{\sum\limits_{(p_i)}\frac{1}{p_i^s}}{\log\left(\frac{1}{s-1}\right)}\right\}$$

existirt, wo die im Zähler stehende Summe über alle Primzahlen p_i zu erstrecken ist, so sagen wir: die Primzahlen von der Art p_i besitzen eine Dichtigkeit; hat jener Limes den Wert Δ_i, so heisse Δ_i die **Dichtigkeit** der Primzahlen von der Art p_i. *Kronecker* macht bei seinen Untersuchungen die unausgesprochene Annahme, dass die Primzahlen von sämtlichen m Arten $p_1, \ldots, p_m$ Dichtigkeiten besitzen. Ob diese Annahme zutrifft, ist bisher nicht entschieden worden. Dagegen gelingt der Nachweis des folgenden Satzes:

Satz 83. Wenn in einem beliebigen Körper $m$ten Grades von den Primzahlen der m Arten $p_1, \ldots p_m$ irgend $m-1$ Arten Dichtigkeiten besitzen, so besitzt auch die übrigbleibende Art eine Dichtigkeit, und die m Dichtigkeiten $\Delta_1, \ldots, \Delta_m$ erfüllen die Relation:

$$\Delta_1 + 2\Delta_2 + \cdots + m\Delta_m = 1.$$

Beweis. Wenn man die zweite der drei in § 27 angegebenen Darstellungen der Functionen $\zeta(s)$ benutzt und den Logarithmus bildet, so ergiebt sich

$$\log \zeta(s) = \sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s} + S,$$

$$S = \tfrac{1}{2} \sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^{2s}} + \tfrac{1}{3} \sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^{3s}} + \cdots,$$

wo die Summen über sämtliche Primideale $\mathfrak{p}$ des Körpers zu erstrecken sind. Bezeichnen wir nun die Primideale ersten Grades allgemein mit $\mathfrak{p}_1$, so wird offenbar

$$(19.) \qquad \sum_{(\mathfrak{p}_1)} \frac{1}{n(\mathfrak{p}_1)^s} = \sum_{(p_1)} \frac{1}{p_1^s} + \sum_{(p_2)} \frac{2}{p_2^s} + \cdots + \sum_{(p_m)} \frac{m}{p_m^s},$$

wo links über alle Primideale $\mathfrak{p}_1$ und rechts bezüglich über alle rationalen Primzahlen $p_1, p_2, \ldots, p_m$ zu summiren ist.

Wir berücksichtigen andererseits, dass für alle Primideale $\mathfrak{p}$ von höherem als dem ersten Grade $n(\mathfrak{p}) \geqq p^2$ ist, und dass eine beliebige Primzahl p höchstens m Primideale enthält; dadurch ergiebt sich:

$$\sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s} - \sum_{(\mathfrak{p}_1)} \frac{1}{n(\mathfrak{p}_1)^s} \leqq m \sum_{(p)} \frac{1}{p^{2s}} < m \sum \frac{1}{h^2},$$

wo die letzte Summe über alle ganzen rationalen Zahlen $h > 1$ zu er-

strecken ist. Desgleichen findet man:

$$S < m\left\{\sum_{(h)} \frac{1}{h^2} + \sum_{(h)} \frac{1}{h^3} + \cdots\right\} = m \sum_{(h)} \frac{1}{h(h-1)} = m.$$

Aus diesen Ungleichungen folgt, dass $\log\zeta(s) - \sum_{(\mathfrak{p}_1)} \frac{1}{n(\mathfrak{p}_1)^s}$ sich für $s=1$ einer endlichen Grenze nähert. Nach Satz 56 hat auch der Ausdruck $\log\zeta(s) - \log\frac{1}{s-1}$ für $s=1$ einen endlichen Grenzwert, und daher gilt das Nämliche auch von dem Ausdruck

$$\sum_{(\mathfrak{p}_1)} \frac{1}{n(\mathfrak{p}_1)^s} - \log\frac{1}{s-1},$$

d. h. es ist

$$\underset{s=1}{L}\ \frac{\sum\limits_{(\mathfrak{p}_1)} \frac{1}{n(\mathfrak{p}_1)^s}}{\log\frac{1}{s-1}} = 1,$$

woraus unter Benutzung der Formel (19.) die Behauptung folgt.

Für einen Galois'schen Körper K vom Mten Grade ist $\varDelta_1 = 0$, $\varDelta_2 = 0, \ldots, \varDelta_{M-1} = 0$, und daher folgt aus Satz 83:

Satz 84. In einem Galois'schen Körper Mten Grades besitzen die in lauter Primideale ersten Grades zerfallenden Primzahlen p_M eine Dichtigkeit, und diese Dichtigkeit ist $\varDelta_M = \frac{1}{M}$.

Ist k ein beliebiger Körper und K derjenige Galois'sche Körper Mten Grades, welcher aus k und den zu k conjugirten Körpern $k', \ldots, k^{(m-1)}$ zusammengesetzt ist, so stimmen, wie man leicht erkennt, die Primzahlen p_m in k mit den Primzahlen p_M in K überein, und daher besitzen die Primzahlen p_m in k eine Dichtigkeit, und diese ist gleich $\frac{1}{M}$, d. h. gleich dem reciproken Wert des Grades M seiner Galois'schen Resolvente. [*Kronecker*[14].]

Capitel XIII.

Die Zusammensetzung der Zahlkörper.

§ 51.

Der aus einem Körper und dessen conjugirten Körpern zusammengesetzte Galois'sche Körper.

Satz 85. Wird aus den beiden Körpern k_1 und k_2 ein Körper K zusammengesetzt, so enthält die Discriminante des zusammengesetzten Körpers K alle und nur diejenigen rationalen Primzahlen als Factoren, welche in der Discriminante von k_1 oder in derjenigen von k_2 oder in beiden aufgehen.

Der Beweis dieses Satzes ergiebt sich aus Satz 39. Eine unmittelbare Folge des Satzes 85 ist die weitere Thatsache:

Satz 86. Wenn man aus dem Körper k vom $m$ten Grade und den sämtlichen zu ihm conjugirten Körpern $k', \ldots, k^{(m-1)}$ einen Galois'schen Körper K zusammensetzt, so enthält die Discriminante dieses Körpers K alle und nur diejenigen rationalen Primzahlen, welche in der Discriminante des Körpers k aufgehen.

§ 52.

Die Zusammensetzung zweier Körper, deren Discriminanten zu einander prim sind.

Ein besonderes Interesse beansprucht der Fall, dass die Discriminante der zusammenzusetzenden Körper zu einander prim sind. Der wichtigste und fruchtbarste Satz über diesen Fall ist der folgende:

Satz 87. Zwei Körper k_1 und k_2 bezüglich von den Graden m_1 und m_2, deren Discriminanten zu einander prim sind, ergeben durch Zusammensetzung stets einen Körper vom Grade $m_1 m_2$.

Beweis. Der aus k_1 und den sämtlichen zu k_1 conjugirten Körpern zusammengesetzte Galois'sche Körper werde mit K_1 bezeichnet; die Discriminante von K_1 ist nach Satz 86 prim zu der Discriminante von k_2. Es sei ϑ eine den Körper k_1 bestimmende Zahl; dieselbe genügt einer irreduciblen Gleichung $m$ten Grades mit ganzen rationalen Coefficienten.

Wäre nun der aus k_1 und k_2 zusammengesetzte Körper von niederem als dem $(m_1 m_2)$ten Grade, so müsste diese Gleichung im Rationalitätsbereich k_2 reducibel werden, d. h. die Zahl ϑ würde dann einer Glei-

chung von der Gestalt

$$\vartheta^r + \alpha_1 \vartheta^{r-1} + \cdots + \alpha_r = 0$$

genügen, deren Grad $r < m_1$ ist, und deren Coefficienten $\alpha_1, \ldots, \alpha_r$ Zahlen in k_2 sind. Der aus diesen Coefficienten $\alpha_1, \ldots, \alpha_r$ zusammengesetzte Zahlkörper werde k genannt. Da $\alpha_1, \ldots, \alpha_r$ sich durch die r Wurzeln der obigen Gleichung rational ausdrücken lassen, so ist k ein Unterkörper von K_1, und da k auch zugleich ein Unterkörper von k_2 ist, so müsste die Discriminante von k nach Satz 39 sowohl in der Discriminante von k_1 als auch in derjenigen von k_2 als Factor enthalten sein; hieraus würde für die Discriminante dieses Körpers k der Wert 1 folgen, und dieser Umstand widerspricht dem Satze 44.

Wir heben noch folgende Thatsachen hervor, deren Richtigkeit nunmehr leicht erkannt wird:

Satz 88. Wenn k_1, k_2 zwei Körper bezüglich von den Graden m_1, m_2 und mit den zu einander primen Discriminanten d_1, d_2 sind, so ist die Discriminante des zusammengesetzten Körpers K gleich $d_1^{m_2} d_2^{m_1}$. Die $m_1 m_2$ Zahlen einer Basis des Körpers K erhält man, wenn man jede der m_1 Basiszahlen des Körpers k_1 mit jeder der m_2 Basiszahlen des Körpers k_2 multiplicirt. Ist p eine rationale Primzahl, welche in k_1 die Zerlegung $p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ und in k_2 die Zerlegung $p = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ erfährt, wo $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ und $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ von einander verschiedene Primideale bez. in den Körpern k_1 und k_2 bedeuten, so gilt in K die Zerlegung $p = \prod_{i,l} \mathfrak{P}_{il}^{e_i}$, wo das Product über $i = 1, \ldots, r$ und $l = 1, \ldots, s$ zu erstrecken ist und $\mathfrak{P}_{il}$ dasjenige Primideal in K bedeutet, welches als der grösste gemeinsame Teiler der beiden Ideale $\mathfrak{p}_i$ und $\mathfrak{q}_l$ definirt ist.

Werden zwei Körper k_1, k_2 mit beliebigen Discriminanten zu Grunde gelegt, so ist die Beantwortung der entsprechenden Fragen nur unter beschränkenden Annahmen über die Natur der Körper und der zu zerlegenden Primzahlen einfach. [*Hensel*[3].]

Die bisher in Capitel X—XIII dargelegten Resultate scheinen mir die wichtigsten Grundzüge einer Theorie der Ideale und Discriminanten des Galois'schen Körpers zu enthalten. Die befolgten Methoden gestatten noch nach mannigfachen Richtungen eine allgemeinere Ausführung; insbesondere gilt eine Reihe der in § 39—44 bewiesenen Sätze ohne wesentliche Aenderung für relativ Galois'sche Körper. [*Dedekind*[8].]

Capitel XIV.

Die Primideale ersten Grades und der Klassenbegriff.

§ 53.

Die Erzeugung der Idealklassen durch Primideale ersten Grades.

Es ist von hohem Interesse, dass die in Capitel X—XII entwickelten Principien auch über die Frage der Erzeugung und Natur der Idealklassen eines Zahlkörpers neues Licht verbreiten. In diesem und in dem folgenden Capitel werden die wichtigsten auf diese Frage bezüglichen allgemeinen Sätze dargelegt. Der erste Satz betrifft die Erzeugung der Idealklassen eines beliebigen Galois'schen Zahlkörpers durch Primideale ersten Grades und lautet:

Satz 89. In jeder Idealklasse eines Galois'schen Körpers giebt es Ideale, deren Primfactoren sämtlich Ideale ersten Grades sind.

Wir beweisen zunächst den folgenden Hülfssatz:

Hülfssatz 12. Wenn K ein Galois'scher Körper vom Mten Grade mit der Discriminante D ist, und $\mathfrak{P}$ ein in $DM!$ nicht aufgehendes Primideal von einem Grade $f > 1$ in diesem Körper bedeutet, so giebt es stets eine zu $DM!$ prime ganze Zahl Ω in K, welche durch $\mathfrak{P}$, aber nicht durch $\mathfrak{P}^2$ teilbar ist, und deren übrige Primfactoren sämtlich von niederem als dem $f$ten Grade sind.

Beweis. Es sei $\boldsymbol{P}$ eine ganze Zahl des Körpers K von der Art, dass jede andere ganze Zahl Ω einer ganzzahligen Function von $\boldsymbol{P}$ nach $\mathfrak{P}^2$ congruent wird. Nach Satz 29 existirt eine solche Zahl $\boldsymbol{P}$ stets. Wir bezeichnen ferner die zu $\mathfrak{P}$ conjugirten und von $\mathfrak{P}$ verschiedenen Primideale mit $\mathfrak{P}', \mathfrak{P}'', \dots, \mathfrak{P}^{(m)}$ und bestimmen dann eine ganze Zahl A in K, welche den Congruenzen

$$\begin{aligned} A &\equiv \boldsymbol{P}, \quad (\mathfrak{P}^2) \\ A &\equiv 0, \quad (\mathfrak{P}'\mathfrak{P}''\dots\mathfrak{P}^{(m)}) \\ A &\equiv 1, \quad (M!) \end{aligned}$$

genügt. Ist z eine solche Substitution der zu $\mathfrak{P}$ gehörigen Zerlegungsgruppe, für welche $z\boldsymbol{P} \equiv \boldsymbol{P}^p$ nach $\mathfrak{P}$ wird, so sind offenbar die $f-1$ Differenzen $A - zA,\ A - z^2A,\ \dots,\ A - z^{f-1}A$ zu $\mathfrak{P}$ prim. Ist ferner s eine nicht zur Zerlegungsgruppe gehörige Substitution, so wird sA durch $\mathfrak{P}$ teilbar, und folglich ist die Differenz $A - sA$ zu $\mathfrak{P}$ prim. Die Differente von A ist mithin zu $\mathfrak{P}$ prim, und daher folgt nach der Bemerkung auf

S. 180, dass A eine den Körper K bestimmende Zahl darstellt. Mit Rücksicht auf Satz 31 ist K der Trägheitskörper von $\mathfrak{P}$, und daher genügt A einer Gleichung von der Gestalt:

$$A^f + \alpha_1 A^{f-1} + \cdots + \alpha_f = 0,$$

wo $\alpha_1, \ldots, \alpha_f$ Zahlen im Zerlegungskörper k des Primideals $\mathfrak{P}$ bedeuten. Die übrigen Unterkörper des Körpers K vom nämlichen Grade $\frac{M}{f}$ bezeichnen wir mit $k', k'', \ldots$; es genügt A dann auch den Gleichungen

$$A^f + \alpha'_1 A^{f-1} + \cdots + \alpha'_f = 0,$$
$$A^f + \alpha''_1 A^{f-1} + \cdots + \alpha''_f = 0,$$
$$\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot$$

wo $\alpha'_1, \ldots, \alpha'_f$ Zahlen in k', $\alpha''_1, \ldots, \alpha''_f$ Zahlen in k'' u. s. f. sind. Nunmehr bestimme man f ganze rationale Zahlen $a_1, \ldots, a_f$ so, dass

$$a_1 \equiv \alpha_1, \ldots, a_f \equiv \alpha_f, \quad (\mathfrak{P})$$

wird; dies ist möglich, weil nach Satz 70 das Ideal $\mathfrak{P}$ in k vom ersten Grade ist. Sodann seien $b_1 \ldots, b_f$, solche f ganze rationale Zahlen, welche den Congruenzen

$$M!b_1 \equiv a_1, \ldots, M!b_f \equiv a_f, \quad (p)$$

genügen, und für welche überdies keine der zum Index 1 gehörigen Verbindungen

$$\beta_1 = M!b_1 - \alpha_1, \quad \beta'_1 = M!b_1 - \alpha'_1, \quad \ldots$$

verschwindet. Wir setzen ferner

$$B = A^f + M!(b_1 A^{f-1} + b_2 A^{f-2} + \cdots + b_f).$$

Endlich bezeichnen wir die sämtlichen von p verschiedenen und in der Discriminante $\varDelta$ von A oder in den Normen der Zahlen $\beta_1, \beta'_1, \ldots$ aufgehenden rationalen Primzahlen, soweit sie grösser als M sind, mit $q_1, \ldots, q_l$. Ist q_i eine beliebige unter diesen, so muss, da sie in K höchstens M Primfactoren enthalten kann, mindestens eine der $q_i (> M)$ Zahlen B, $B+1$, $B+2, \ldots, B+q_i-1$ zu q_i prim sein; es sei etwa $B+c_i$ prim zu q_i. Bestimmt man dann eine ganze rationale Zahl c, welche den l Congruenzen $M!pc \equiv c_i$ nach q_i für $i = 1, 2, \ldots, l$ genügt, so ist

$$\Omega = B + M!pc$$

eine Zahl von der Eigenschaft, wie sie unser Hülfssatz 12 verlangt.

In der That: wegen der Congruenz $A \equiv 1$ nach $M!$ ist die Zahl Ω prim zu allen denjenigen rationalen Primzahlen, welche $\leqq M$ sind; und andererseits ist Ω auf Grund der Bestimmungsweise der Zahl c prim zu allen denjenigen in A enthaltenen rationalen Primzahlen, welche grösser als M sind. Die Zahl Ω ist daher prim zu den von p verschiedenen, in A aufgehenden rationalen Primzahlen.

Ferner ist Ω teilbar durch $\mathfrak{P}$, aber nicht durch $\mathfrak{P}', \mathfrak{P}'', \ldots, \mathfrak{P}^{(m)}$, da $M! b_f \equiv a_f \not\equiv 0$ nach p wird. Die Zahl Ω ist in der Gestalt

$$\Omega = A^f + m_1 A^{f-1} + \cdots + m_f,$$

darstellbar, wo $m_1, \ldots, m_f$ ganze rationale Zahlen bedeuten. Da $A \equiv P$ nach $\mathfrak{P}^2$ ist und P keiner ganzzahligen Congruenz von niederem als dem $(2f)$ten Grade nach $\mathfrak{P}^2$ genügen kann, so folgt, dass Ω nicht durch $\mathfrak{P}^2$ teilbar ist.

Wäre ferner Ω durch ein Primideal $\mathfrak{Q}$ vom Grade $f' > f$ teilbar, und seien $1, z', z'^2, \ldots, z'^{f'-1}$ die f' Substitutionen der Zerlegungsgruppe von $\mathfrak{Q}$, durch welche diese aus der Trägheitsgruppe erzeugt wird, so müssten die f' Congruenzen

$$A^f + m_1 \quad A^{f-1} + \cdots + m_f \equiv 0, \quad (\mathfrak{Q})$$
$$(z'A)^f + m_1 (z'A)^{f-1} + \cdots + m_f \equiv 0, \quad (\mathfrak{Q})$$
$$\cdots\cdots\cdots\cdots$$

bestehen; diese würden zur Folge haben, dass die Discriminante Δ der Zahl A durch $\mathfrak{Q}$ teilbar ist, was nach dem Obigen nicht zutrifft.

Es sei endlich Ω durch ein Primideal $\mathfrak{Q}$ vom Grade f teilbar; dann müsste einer der Körper $k, k', k'', \ldots$ Zerlegungskörper von $\mathfrak{Q}$ sein; es sei dies etwa der Körper k'. Unter dieser Annahme setze man Ω in die Gestalt

$$\Omega = \Omega - (A^f + \alpha'_1 A^{f-1} + \cdots + \alpha'_f) = \beta'_1 A^{f-1} + \cdots + \beta'_f,$$

wo $\beta'_1, \ldots, \beta'_f$ Zahlen in k' bedeuten. Sind $1, z', z'^2, \ldots, z'^{f-1}$ die f für $\mathfrak{Q}$ zur Erzeugung seiner Zerlegungsgruppe aus seiner Trägheitsgruppe dienenden Substitutionen, so folgt

$$\beta'_1 A^{f-1} + \cdots + \beta'_f \equiv 0, \quad (\mathfrak{Q})$$
$$\beta'_1 (z'A)^{f-1} + \cdots + \beta'_f \equiv 0, \quad (\mathfrak{Q})$$
$$\cdots\cdots\cdots$$

und diese Congruenzen würden zur Folge haben, dass entweder Δ oder

β_1' durch $\mathfrak{Q}$ teilbar ist, womit die obigen Festsetzungen im Widerspruch stehen.

Wenn wir berücksichtigen, dass in jeder Klasse ein Ideal gefunden werden kann, welches zu $DM!$ prim ist, so folgt aus dem somit bewiesenen Hülfssatz 12, wie man leicht sieht, der Satz 89. Derselbe ist für den Fall des Kreiskörpers bereits von *Kummer* bewiesen worden. [*Kummer* [6].]

Capitel XV.

Der relativ cyklische Körper vom Primzahlgrade.

§ 54.

Die symbolische Potenz. Der Satz von den Zahlen mit der Relativnorm 1.

Es soll jetzt über relativ Abel'sche Körper eine Reihe fundamentaler Sätze abgeleitet werden. Um dieselben leichter aussprechen und beweisen zu können, schicken wir einige Bezeichnungen und Festsetzungen voraus.

Es sei K ein Zahlkörper vom Grade lm; derselbe sei relativ-cyklisch in Bezug auf den Körper k vom $m$ten Grade; der Relativgrad l sei eine Primzahl. Die Substitutionen der cyklischen Relativgruppe seien $1, S, S^2, \ldots, S^{l-1}$. Endlich definiren wir den Begriff der **symbolischen Potenz** einer Zahl A des Körpers K, wie folgt: wenn A eine beliebige ganze oder gebrochene Zahl in K ist und $a, a_1, \ldots, a_{l-1}$ irgend welche ganze rationale Zahlen bedeuten, so möge der Ausdruck

$$A^a (SA)^{a_1} (S^2 A)^{a_2} \ldots (S^{l-1} A)^{a_{l-1}}$$

zur Abkürzung mit

$$A^{a+a_1 S+a_2 S^2+\cdots+a_{l-1} S^{l-1}} = A^{F(S)}$$

bezeichnet werden, wo $F(S)$ die auf der linken Seite im Exponenten von A stehende ganzzahlige Function von S bedeutet. Die symbolische $F(S)$te Potenz von A stellt hiernach stets wiederum eine ganze oder gebrochene Zahl des Körpers K dar. Diese symbolische Potenzirung kann

als Verallgemeinerung einer Bezeichnungsweise angesehen werden, welche *Kronecker* im Falle des Kreiskörpers eingeführt hat. [*Kronecker*[1].]

Wir beweisen nun der Reihe nach folgende Eigenschaften des relativ-cyklischen Körpers K:

Satz 90. Jede ganze oder gebrochene Zahl A in K, deren Relativnorm in Bezug auf k gleich 1 ist, wird die symbolische $(1-S)$te Potenz einer gewissen ganzen Zahl B des Körpers K.

Beweis. Es sei x eine Veränderliche und Θ eine den Körper K bestimmende Zahl; dann setze man:

$$A_x = \frac{x+\Theta}{x+S\Theta} A = (x+\Theta)^{1-S} A$$

und

$$B_x = 1 + A_x^1 + A_x^{1+S} + A_x^{1+S+S^2} + \cdots + A_x^{1+S+S^2+\cdots+S^{l-2}}.$$

Berücksichtigt man, dass nach Voraussetzung $A^{1+S+\cdots+S^{l-1}} = 1$ ist und folglich auch $A_x^{1+S+\cdots+S^{l-1}} = 1$ wird, so ergiebt sich $B_x^{1-S} = A_x$. Da B_x eine rationale Function von x ist, welche, wie leicht ersichtlich, nicht identisch für alle x verschwindet, so kann man eine ganze rationale Zahl $x = a$ so wählen, dass B_a eine von 0 verschiedene Zahl in K wird. Die Zahl $B^* = \frac{B_a}{a+\Theta}$ genügt dann der Gleichung $A = B^{*1-S}$. Setzen wir $B^* = \frac{B}{b}$, wo B eine ganze algebraische Zahl in K und b eine ganze rationale Zahl bedeutet, so ist auch $A = B^{1-S}$.

§ 55.

Das System von relativen Grundeinheiten und der Nachweis ihrer Existenz.

Ein zweiter wichtiger Satz über den Körper K betrifft eine Eigenschaft der Einheiten in K. Kommen unter den m conjugirten Körpern, welche durch k bestimmt sind, r_1 reelle Körper und r_2 Paare conjugirt imaginärer Körper vor, so ist nach Satz 47 die Zahl der Grundeinheiten in k gleich $r = r_1 + r_2 - 1$. Wir definiren nun den Begriff eines **Systems von relativen Grundeinheiten** des Körpers K bezüglich k. Unter einem solchen System verstehen wir ein System von $r+1$ Einheiten $H_1, \ldots, H_{r+1}$ im Körper K von der Eigenschaft, dass eine Einheit von der Gestalt $H_1^{F_1(S)} \ldots H_{r+1}^{F_{r+1}(S)}[\varepsilon]$ nur dann die symbolische $(1-S)$te Potenz einer Einheit in K werden kann, wenn die ganzen alge-

braischen Zahlen $F_1(\zeta), \ldots, F_{r+1}(\zeta)$ sämtlich durch $1-\zeta$ teilbar sind. Dabei bedeuten $F_1(S), \ldots, F_{r-1}(S)$ ganzzahlige Functionen von S; $[\varepsilon]$ bedeutet eine beliebige Einheit des Körpers k oder eine solche Einheit des Körpers K, deren $l$te Potenz eine Einheit in k ist; ζ endlich bedeutet eine von 1 verschiedene $l$te Einheitswurzel.

Satz 91. Wenn der Relativgrad l des relativ-cyklischen Körpers K in Bezug auf den Körper k eine ungerade Primzahl ist, so existirt in K stets ein System von $r+1$ relativen Grundeinheiten, wobei r für k die Bedeutung wie in Satz 47 hat.

Beweis. Wegen $l \neq 2$ kommen unter den lm durch K bestimmten conjugirten Körpern lr_1 reelle Körper und lr_2 imaginäre Paare von Körpern vor. Es sei $\varepsilon_1, \ldots, \varepsilon_r$ ein System von $r = r_1 + r_2 - 1$ Grundeinheiten des Körpers k. Man wähle unter den Einheiten in K eine solche Einheit E_1 aus, dass $E_1, \varepsilon_1, \ldots, \varepsilon_r$ ein System von unabhängigen Einheiten bilden; dann müssen auch die $r+l-1$ Einheiten $E_1, E_1^S, \ldots, E_1^{S^{l-2}}, \varepsilon_1, \ldots, \varepsilon_r$ ein System unabhängiger Einheiten sein.

Zum Beweise hierfür machen wir die gegenteilige Annahme und denken uns $E_1^{F(S)} = \varepsilon^*$, wo $F(S)$ eine nicht identisch verschwindende ganzzahlige Function vom $(l-2)$ten Grade in S und ε^* eine Einheit des Körpers k bedeutet. Da die Function $1+S+\cdots+S^{l-1}$ irreducibel ist, (vergl. die Bemerkung am Schluss des § 91), so lassen sich zwei ganzzahlige Functionen G_1, G_2 von S und eine von 0 verschiedene ganze rationale Zahl a derart bestimmen, dass

$$FG_1 + (1+S+\cdots+S^{l-1})G_2 = a$$

wird. Hieraus folgt unter Berücksichtigung von

$$E_1^{1+S+\cdots+S^{l-1}} = \varepsilon^{**}$$

die Gleichung $E_1^a = \varepsilon^{***}$, welche unserer Annahme zuwider läuft; dabei bedeuten ε^{**} und ε^{***} Einheiten in k.

Nunmehr wähle man eine Einheit E_2 so, dass $E_2, E_1, E_1^S, \ldots, E_1^{S^{l-2}}$, $\varepsilon_1, \ldots, \varepsilon_r$ ein System unabhängiger Einheiten bilden, und beweise dann in ähnlicher Weise, wie vorher, dass auch die Einheiten $E_2, E_2^S, \ldots, E_2^{S^{l-2}}$, $E_1, E_1^S, \ldots, E_1^{S^{l-2}}, \varepsilon_1, \ldots, \varepsilon_r$ unabhängige Einheiten sind. So fortfahrend, gelangen wir zu $r_1 + r_2 = r+1$ Einheiten $E_1, \ldots, E_{r+1}$ von der Beschaffenheit, dass die Einheiten

$$E_i, \quad E_i^S, \quad \ldots, \quad E_i^{S^{l-2}}, \quad \varepsilon_1, \quad \ldots, \quad \varepsilon_r \qquad (i=1,2,\ldots,r+1)$$

ein System von unabhängigen Einheiten bilden. Die Zahl dieser Einheiten beträgt

$$(r+1)(l-1)+r = lr_1+lr_2-1.$$

Es sei nun l^m eine so hohe Potenz von l, dass ein Ausdruck

$$(20.) \qquad E_1^{F_1(S)} \quad . \; . \; . \quad E_{r+1}^{F_{r+1}(S)}[\varepsilon],$$

in welchem $F_1(S), \ldots, F_{r+1}(S)$ beliebige ganzzahlige Functionen vom $(l-2)$ten Grade in S bedeuten und $[\varepsilon]$ die auf S. 272 erklärte Bedeutung hat, nicht anders eine l^mte Potenz einer Einheit in K werden kann, als wenn alle Coefficienten der $r+1$ Functionen $F_1(S), \ldots, F_{r+1}(S)$ durch l teilbar sind. Dass es eine solche Potenz l^m stets geben muss, folgt, wenn man die lr_1+lr_2-1 nach Satz 47 existirenden Grundeinheiten des Körpers K zu Hülfe zieht.

Wir berücksichtigen ferner die Identität

$$(1-S)^l = 1-S^l+l\,G(S),$$

in der G eine ganzzahlige Function bedeutet; da hiernach die $(1-S)^{l^m}$te symbolische Potenz einer Zahl in K zugleich auch eine l^mte wirkliche Potenz ist, so folgt, dass der Ausdruck (20.) nicht anders die $(1-S)^{l^m}$te symbolische Potenz einer Einheit werden kann, als wenn die ganzen algebraischen Zahlen $F_1(\zeta), \ldots, F_{r+1}(\zeta)$ sämtlich durch $1-\zeta$ teilbar sind.

Es sei nun e_1 die grösste ganze rationale Zahl $\geqq 0$ von der Art, dass ein Ausdruck von der Gestalt (20.) eine $(1-S)^{e_1}$te symbolische Potenz einer Einheit ist, ohne das sämtliche Zahlen $F_1(\zeta), \ldots, F_{r+1}(\zeta)$ durch $1-\zeta$ teilbar sind; wir nehmen an, es sei ein solcher Ausdruck:

$$E_1^{F_1(S)} \ldots E_{r+1}^{F_{r+1}(S)}[\varepsilon] = H_1^{(1-S)^{e_1}},$$

wo $F_1(S), \ldots, F_{r+1}(S)$ gewisse ganze rationale Functionen von S sind und etwa $F_1(\zeta)$ nicht durch $1-\zeta$ teilbar sein möge; $[\varepsilon]$ hat die frühere Bedeutung, und H_1 ist eine gewisse Einheit des Körpers K. Des weiteren nehmen wir an, es sei e_2 die grösste ganze Zahl $\geqq 0$ von der Beschaffenheit, dass ein entsprechend aus den Einheiten $E_2, \ldots, E_{r+1}$ gebildeter Ausdruck existirt, der die $(1-S)^{e_2}$te symbolische Potenz einer Einheit in K wird; es sei etwa ein solcher Ausdruck:

$$E_2^{F_2(S)} \ldots E_{r+1}^{F_{r+1}(S)}[\varepsilon] = H_2^{(1-S)^{e_2}},$$

wo $F_2(S), \ldots, F_{r+1}(S)$ wiederum gewisse ganze rationale Functionen

von S sind und etwa $F_2(\zeta)$ nicht durch $1-\zeta$ teilbar sein möge; $\boldsymbol{H}_2$ bedeutet eine Einheit in K. So fortfahrend, gelangen wir zu $r+1$ Einheiten $\boldsymbol{H}_1, \boldsymbol{H}_2, \ldots, \boldsymbol{H}_{r+1}$; dieselben bilden ein System von relativen Grundeinheiten des Körpers K.

Um dies zu zeigen, nehmen wir im Gegenteil an, es gäbe $r+1$ ganze rationale Functionen $G_1(S), \ldots, G_{r+1}(S)$ derart, dass

$$\boldsymbol{H}_1^{G_1(S)} \ldots \boldsymbol{H}_{r+1}^{G_{r+1}(S)}[\varepsilon] = \boldsymbol{Z}^{1-S}$$

wird, wo $\boldsymbol{Z}$ eine Einheit in K bedeutet; es sei ferner unter den Zahlen $G_1(\zeta), \ldots, G_{r+1}(\zeta)$ etwa $G_h(\zeta)$ die erste nicht durch $1-\zeta$ teilbare Zahl: dann wäre offenbar auch der Teil

$$\boldsymbol{H}_h^{G_h(S)} \boldsymbol{H}_{h+1}^{G_{h+1}(S)} \ldots \boldsymbol{H}_{r+1}^{G_{r+1}(S)}[\varepsilon]$$

des letzten Products die $(1-S)$te symbolische Potenz einer Einheit des Körpers K. Da aber in der Reihe der Zahlen $e_1, e_2, \ldots, e_{r+1}$ keine folgende grösser ist als die vorhergehende, so stossen wir, wenn wir den letzten Ausdruck in die $(1-S)^{e_h}$te Potenz erheben und dann wieder die Einheiten $\boldsymbol{E}_h, \ldots, \boldsymbol{E}_{r+1}$ einführen, auf einen Widerspruch mit unseren Festsetzungen.

Der eben bewiesene Satz 91 gilt, wie leicht ersichtlich, auch für $l=2$, wenn in diesem Falle noch der Umstand hinzukommt, dass unter den durch K bestimmten $2m$ einander conjugirten Körpern doppelt so viel reelle Körper als unter den durch k bestimmten m conjugirten Körpern vorhanden sind.

§ 56.

Die Existenz einer Einheit in K, welche die Relativnorm 1 besitzt und doch nicht dem Quotienten zweier relativ-conjugirten Einheiten gleich wird.

Satz 92. Falls der Relativgrad l des relativ-cyklischen Körpers K in Bezug auf den Körper k eine ungerade Primzahl ist, giebt es in K stets eine Einheit $\boldsymbol{H}$, deren Relativnorm in Bezug auf k gleich 1 ausfällt, und welche doch nicht die symbolische $(1-S)$te Potenz von einer Einheit des Körpers K ist.

Beweis. Wir nehmen zunächst an, dass der Körper k nicht die $l$te Einheitswurzel ζ enthält. Es seien $\eta_1, \ldots, \eta_{r+1}$ irgend $r+1$ Einheiten in k; dann folgt, dass es stets $r+1$ ganze rationale Zahlen $a_1, \ldots, a_{r+1}$ giebt, welche nicht sämtlich durch l teilbar sind, und für

welche $\eta_1^{a_1} \ldots \eta_{r+1}^{a_{r+1}} = 1$ wird. In der That, wären in einer Gleichung von der letzteren Gestalt die Exponenten $a_1, \ldots, a_{r+1}$ sämtlich durch l teilbar, so müsste $\eta_1^{\frac{a_1}{l}} \ldots \eta_{r+1}^{\frac{a_{r+1}}{l}}$ eine $l$te Einheitswurzel und demnach infolge der Voraussetzung $= 1$ sein; hieraus ergiebt sich durch Wiederholung des Verfahrens das Gesagte. Nehmen wir nun $\eta_1, \ldots, \eta_{r+1}$ gleich den Relativnormen von $H_1, \ldots, H_{r+1}$, wo $H_1, \ldots, H_{r+1}$ ein System von relativen Grundeinheiten in K sind, und setzen dann $H = H_1^{a_1} \ldots H_{r+1}^{a_{r+1}}$, so folgt $N_k(H) = H^{1+S+S^2+\cdots+S^{l-1}} = 1$ und daher nach dem Satz 90: $H = A^{1-S}$; da $H_1, \ldots, H_{r+1}$ relative Grundeinheiten sind, so ist die Zahl A keine Einheit.

Um den Satz 92 allgemein zu beweisen, werde angenommen, dass k die primitive l^hte Einheitswurzel ζ', aber nicht die primitive l^{h+1}te Einheitswurzel enthielte. Durch ein ähnliches Verfahren, wie das oben angewandte, wird erkannt, dass, wenn $\eta_1, \ldots, \eta_{r+2}$ irgend welche $r+2$ Einheiten in k sind, stets eine ganze rationale Zahl a und ferner $r+2$ ganze rationale, nicht sämtlich durch l teilbare Zahlen $a_1, \ldots, a_{r+2}$ von der Art gefunden werden können, dass

$$\eta_1^{a_1} \ldots \eta_{r+2}^{a_{r+2}} = \zeta'^{al}$$

ist.

Andererseits bedenke man, dass die Relativnorm

$$N_k(\zeta) = \zeta^{1+S+S^2+\cdots+S^{l-1}} = 1$$

wird und daher nach Satz 90 ζ eine $(1-S)$te symbolische Potenz werden muss. Gäbe es nun keine Einheit E in K, so dass $\zeta = E^{1-S}$ ist, so wäre bereits ζ eine Zahl von der gewünschten Beschaffenheit. Im anderen Falle folgt $E^{l(1-S)} = 1$, d. h. $E^l = SE^l$, und daher stellt E^l eine Einheit ε in k dar, während E selbst gewiss nicht in k liegt. Wegen $E = \sqrt[l]{\varepsilon}$ ergiebt sich $N_k(E) = E^l = \varepsilon$. Es sei $H_1, \ldots, H_{r+1}$ ein System von relativen Grundeinheiten in K; wir setzen nun:

$$\eta_1 = N_k(H_1), \quad \ldots, \quad \eta_{r+1} = N_k(H_{r+1}), \quad \eta_{r+2} = N_k(E) = E^l,$$
$$H = H_1^{a_1} \ldots H_{r+1}^{a_{r+1}} E^{a_{r+2}} \zeta'^{-a} = H_1^{a_1} \ldots H_{r+1}^{a_{r+1}} [\varepsilon],$$

wo $a, a_1, \ldots, a_{r+2}$ die vorhin bestimmten Zahlen sind und $[\varepsilon]$ die $l$te Wurzel aus einer Einheit des Körpers k bedeutet; dann wird $N_k(H) = 1$. Die Zahlen $a_1, \ldots, a_{r+1}$ können nicht sämtlich durch l teilbar sein.

Denn aus

$$\left(\eta_1^{\frac{a_1}{l}} \cdots \eta_{r+1}^{\frac{a_{r+1}}{l}} E^{a_{r+2}} \zeta'^{-a}\right)^l = 1$$

würde dann

$$\eta_1^{\frac{a_1}{l}} \cdots \eta_{r+1}^{\frac{a_{r+1}}{l}} E^{a_{r+2}} \zeta'^{-a} = \zeta^b$$

folgen, wo b eine ganze rationale Zahl bedeutet. Da a_{r+2} bei unserer Annahme nicht auch durch l teilbar sein darf, so würde aus der letzten Gleichung folgen, dass E in k liegt, was nicht zutrifft. Die Einheit H erfüllt daher alle Bedingungen des Satzes 92.

Die Sätze 90, 91 und 92 sind zum Teil und in anderer Form bereits von *Kummer* für den Fall bewiesen worden, dass der Unterkörper k der durch ζ bestimmte Kreiskörper $(l-1)$ten Grades ist. [*Kummer*[14, 20, 21].]

§ 57.

Die ambigen Ideale und die Relativdifferente des relativ-cyklischen Körpers K.

Wenn ein Ideal $\mathfrak{A}$ des relativ-cyklischen Körpers K bei Anwendung der Substitution S ungeändert bleibt und überdies keinen Factor enthält, welcher ein Ideal in k ist, so heisst $\mathfrak{A}$ ein **ambiges Ideal.** Insbesondere heisst ein Primideal des Körpers K, wenn dasselbe bei Anwendung der Substitution S ungeändert bleibt und nicht zugleich im Körper k liegt, ein **ambiges Primideal.**

Satz 93. Die Relativdifferente des relativ-cyklischen Körpers K in Bezug auf k enthält alle und nur diejenigen Primideale $\mathfrak{P}$, welche ambig sind.

Beweis. Ist $\mathfrak{P}$ ein ambiges Ideal, so wird seine Relativnorm $N_k(\mathfrak{P}) = \mathfrak{P}^l$. Da nicht eine niedere Potenz von $\mathfrak{P}$ in k liegen kann, so ist $\mathfrak{P}^l = \mathfrak{p}$ ein Primideal in k. Umgekehrt, wenn ein Primideal $\mathfrak{p}$ in k gleich der $l$ten Potenz eines Ideals $\mathfrak{P}$ in K wird, so ist $\mathfrak{P}$ ein ambiges Primideal.

Wir unterscheiden nun dreierlei Arten von Primidealen $\mathfrak{p}$ des Körpers k: erstens solche, die der $l$ten Potenz eines Primideals $\mathfrak{P}$ in K gleich sind; zweitens solche, die in l von einander verschiedene Primideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_l$ des Körpers K zerfallen, und drittens solche, die auch in K Primideale sind.

Liegt der erste Fall vor, so setzen wir die Norm $N(\mathfrak{P}) = p^f$; hieraus folgt $N(\mathfrak{p}) = N(\mathfrak{P}^l) = p^{lf}$, und mithin ist die Norm $n(\mathfrak{p})$ des

Primideals $\mathfrak{p}$ im Körper k ebenfalls gleich p^f. Die Gleichheit der Normen $N(\mathfrak{P})$ und $n(\mathfrak{p})$ lässt die Thatsache erkennen, dass eine jede ganze Zahl des Körpers K einer gewissen ganzen Zahl des Körpers k nach $\mathfrak{P}$ congruent ist; aus diesem Umstande erkennt man leicht, dass die Relativdifferente von K in Bezug auf k notwendig durch $\mathfrak{P}$ teilbar ist.

Im zweiten Falle lässt sich in K stets eine ganze Zahl A finden, welche nicht durch $\mathfrak{P}_i$, wohl aber durch alle übrigen $l-1$ Primideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_{i-1}, \mathfrak{P}_{i+1}, \ldots, \mathfrak{P}_l$ teilbar ist, und aus diesem Umstande folgt, dass die Relativdifferente der Zahl A und daher auch die des Körpers K nicht durch $\mathfrak{P}_i$ teilbar ist.

Was endlich die Primideale $\mathfrak{p}$ der dritten Art angeht, so sei P eine Primitivzahl nach dem Primideal $\mathfrak{p}$ in K und ϱ eine Primitivzahl nach $\mathfrak{p}$ in k, und zugleich sei P eine den Körper K bestimmende Zahl. Es genügt dann P einer Gleichung $l$ten Grades von der Gestalt:

$$F(P) = P^l + \alpha_1 P^{l-1} + \cdots + \alpha_l = 0,$$

deren Coefficienten $\alpha_1, \ldots, \alpha_l$ ganze Zahlen in k sind. Wir setzen

$$\alpha_1 \equiv f_1(\varrho), \quad \ldots, \quad \alpha_l \equiv f_l(\varrho), \quad (\mathfrak{p})$$

wo $f_1(\varrho), \ldots, f_l(\varrho)$ ganzzahlige Functionen von ϱ sind, und erhalten so für P die Congruenz:

$$F(P) \equiv P^l + f_1(\varrho) P^{l-1} + \cdots + f_l(\varrho) \equiv 0, \quad (\mathfrak{p}).$$

Da wegen $N(\mathfrak{p}) = (n(\mathfrak{p}))^l$ die Anzahl der in K vorhandenen, nach $\mathfrak{p}$ incongruenten ganzen Zahlen gleich der $l$ten Potenz der Anzahl der in k vorhandenen, nach $\mathfrak{p}$ incongruenten ganzen Zahlen ist, so kann P keiner Congruenz niederen als $l$ten Grades von der nämlichen Art genügen, und daher ist notwendig $\dfrac{\partial F(P)}{\partial P} \not\equiv 0$ nach $\mathfrak{p}$; d. h. die Relativdifferente der Zahl P ist nicht durch $\mathfrak{p}$ teilbar. Durch diese Betrachtungen ist gezeigt, dass die Relativdifferente des Körpers K stets prim zu den Primidealen der zweiten und dritten Art ist, und hieraus ergiebt sich die Richtigkeit des Satzes 93.

§ 58.

Der Fundamentalsatz von den relativ-cyklischen Körpern mit der Relativdifferente 1. Die Bezeichnung dieser Körper als Klassenkörper.

Die Sätze 90, 92 und 93 ermöglichen uns die Erkenntnis einer Thatsache, welche für die Theorie der Zahlkörper von weittragender Bedeutung ist. Diese Thatsache ist folgende:

Satz 94. Wenn der relativ-cyklische Körper K von ungeradem Primzahl-Relativgrade l die Relativdifferente 1 in Bezug auf k besitzt, so giebt es stets in k ein Ideal $\mathfrak{j}$, welches nicht Hauptideal in k ist, wohl aber ein Hauptideal in K wird. Die $l$te Potenz dieses Ideals $\mathfrak{j}$ ist dann notwendig auch in k ein Hauptideal, und die Klassenanzahl des Körpers k ist mithin durch l teilbar.

Beweis. Nach Satz 92 giebt es eine Einheit H mit der Relativnorm 1, welche nicht die $(1-S)$te Potenz einer Einheit ist. Nach Satz 90 ist $H = A^{1-S}$, wo A eine ganze Zahl in K bedeutet; d. h. es ist $A = H.SA$. Für das Hauptideal $\mathfrak{A} = (A)$ folgt hieraus $\mathfrak{A} = S\mathfrak{A}$. Das Ideal $\mathfrak{A}$ liegt im Körper k. Denn ist $\mathfrak{P}$ irgend ein in $\mathfrak{A}$ aufgehendes Primideal des Körpers K, welches nicht in k liegt, so ist nach Satz 93, da wegen der Voraussetzung die Relativdiscriminante keine Teiler besitzt, $\mathfrak{P} \neq S\mathfrak{P}$, und folglich enthält A auch die Relativnorm $N_k(\mathfrak{P})$, welche ein in k liegendes Primideal ist. Das Ideal A ist kein Hauptideal im Körper k; denn in diesem Falle wäre $A = H^* \alpha$, wo H^* eine Einheit und α eine Zahl in k bedeutet; hieraus würde $H = H^{*\,1-S}$ folgen, was dem Obigen widerstreitet. Damit ist der erste Teil des Satzes 94 bewiesen.

Da $N_k(A) = \alpha$ eine Zahl in k und folglich $N_k(\mathfrak{A}) = \mathfrak{A}^l = (\alpha)$ ein Hauptideal in k ist, so haben wir damit den vollständigen Beweis des Satzes 94 erbracht.

Die Sätze 92 und 94 gelten ebenfalls für $l = 2$ unter der oben auf S. 275 am Schluss von § 55 angegebenen Beschränkung.

Es bietet keine erheblichen principiellen Schwierigkeiten dar, den Satz 94 für solche relativ-Abel'sche Körper K mit der Relativdifferente 1 zu verallgemeinern, deren Relativgrad l eine zusammengesetzte Zahl ist.

Wegen der engen Beziehung, die nach Satz 94 der Körper K zu gewissen Idealklassen des Körpers k aufweist, werde K ein **Klassenkörper des Körpers** k genannt.

Dritter Teil.

Der quadratische Zahlkörper.

Capitel XVI.

Die Zerlegung der Zahlen im quadratischen Körper.

§ 59.

Die Basis und die Discriminante des quadratischen Körpers.

Es bedeute m eine ganze rationale, positive oder negative Zahl, die durch keine Quadratzahl ausser 1 teilbar und auch von $+1$ verschieden ist; die quadratische Gleichung

$$x^2 - m = 0$$

ist dann im Bereich der rationalen Zahlen irreducibel. Wir verstehen im Folgenden unter $\sqrt{m}$ stets im Falle $m > 0$ die positive Wurzel jener quadratischen Gleichung und im Falle $m < 0$ diejenige ihrer Wurzeln, welche positiv imaginär ist. Die so festgelegte algebraische Zahl $\sqrt{m}$ bestimmt einen quadratischen reellen, bezüglich imaginären Zahlkörper, der $k(\sqrt{m})$ oder auch schlechthin k heisse; dieser Körper ist stets ein Galois'scher Körper. Durch die Operation der Vertauschung von $\sqrt{m}$ mit $-\sqrt{m}$ in einer Zahl oder einem Ideal des Körpers k geht man zu der conjugirten Zahl bez. dem conjugirten Ideal über. Dieser Uebergang werde durch Vorsetzung des Substitutionszeichens s angedeutet.

Unsere erste Aufgabe ist die Aufstellung einer Basis des quadratischen Körpers und die Ermittelung seiner Discriminante. [*Dedekind*[1].]

Satz 95. Eine Basis des quadratischen Körpers k bilden die Zahlen

1, ω, wenn

$$\omega = \frac{1+\sqrt{m}}{2}, \text{ bez. } \omega = \sqrt{m}$$

genommen wird, je nachdem die Zahl $m \equiv 1$ nach 4 ist oder nicht. Die Discriminante von k ist, entsprechend diesen zwei Fällen,

$$d = m, \text{ bez. } d = 4m.$$

Beweis. Die Zahl ω ist stets ganz, da sie der Gleichung

$$(21.) \qquad x^2 - x - \frac{m-1}{4} = 0, \text{ bez. } x^2 - m = 0$$

genügt. Bezeichnet $\omega' = s\omega$ die zu ω conjugirte Zahl, so ist $d = (\omega - \omega')^2$ die Discriminante der Zahl ω. Nach § 3 S. 180 ist daher jede ganze Zahl des Körpers k in der Gestalt

$$\alpha = \frac{u + v\omega}{d}$$

darstellbar, wo u, v ganze rationale Zahlen sind.

Im Falle, dass $m \equiv 1$ nach 4 ist, schliessen wir aus der Congruenz $2\alpha m = 2u + v + v\sqrt{m} \equiv 0$ nach m, dass $2u + v$ durch $\sqrt{m}$ teilbar sein und folglich auch die Congruenz $2u + v \equiv 0$ nach m gelten muss. Die letztere Congruenz in Verbindung mit der ersteren hat wiederum $v\sqrt{m} \equiv 0$ nach m zur Folge, d. h. v muss durch $\sqrt{m}$ und daher notwendig auch durch m teilbar sein. Da mithin die ganzen rationalen Zahlen u, v beide durch $m = d$ teilbar sind, so ist die im Nenner des obigen Ausdrucks für α stehende Zahl d hebbar.

Ist andererseits $m \not\equiv 1$ nach 4, so schliessen wir aus der Congruenz $4\alpha m = u + v\sqrt{m} \equiv 0$ nach m, wie vorhin, dass sowohl u wie v durch m teilbar sein muss und mithin jedenfalls m in Zähler und Nenner des Ausdrucks für α hebbar ist. Wir erhalten dadurch $\alpha = \frac{u' + v'\sqrt{m}}{4}$, wo u', v' ganze rationale Zahlen bedeuten. Man erkennt aber leicht durch Bildung der Norm $\alpha . s\alpha$, sowohl für $m \equiv 2$ als auch für $m \equiv 3$ nach 4, dass ein Ausdruck $u' + v'\sqrt{m}$ mit ganzen rationalen Zahlen u', v' nur dann durch 2 teilbar sein kann, wenn u', v' beide gerade sind. Wendet man dieses auf 4α und sodann wieder auf 2α an, so zeigt sich, dass auch im Falle $m \not\equiv 1$ nach 4 eine jede ganze Zahl des Körpers k in der Gestalt $u + v\omega$ mit ganzen rationalen Zahlen u, v darstellbar ist.

Der zweite Teil des Satzes ergiebt sich aus der Formel:

$$d = \begin{vmatrix} 1, & \omega \\ 1, & \omega' \end{vmatrix}^2 = (\omega - \omega')^2,$$

durch welche nach § 3 die Discriminante des Körpers definirt wird.

§ 60.

Die Primideale des quadratischen Körpers.

Das Problem der Zerlegung der rationalen Primzahlen in Primideale des Körpers k wird durch folgenden Satz zur vollständigen Erledigung gebracht:

Satz 96. Jede in d aufgehende rationale Primzahl l ist gleich dem Quadrat eines Primideals in k. Jede ungerade, in d nicht aufgehende rationale Primzahl p zerfällt in k entweder in das Product zweier verschiedener, zu einander conjugirter Primideale ersten Grades $\mathfrak{p}$ und $\mathfrak{p}'$ oder stellt selbst ein Primideal zweiten Grades vor, je nachdem d quadratischer Rest oder Nichtrest für p ist. Die Primzahl 2 ist im Falle $m \equiv 1$ nach 4 in k in ein Product zweier von einander verschiedener conjugirter Primideale zerlegbar oder selber Primideal, je nachdem $m \equiv 1$ oder $\equiv 5$ nach 8 ausfällt.

Beweis. Der erste Teil dieser Behauptung, welcher sich auf die in d aufgehenden Primzahlen l bezieht, ist eine Folge des allgemeinen Satzes 31. Ist l eine in d aufgehende ungerade Primzahl, so finden wir

$$l = \mathfrak{l}^2,$$

wo $\mathfrak{l} = (l, \sqrt{m})$ ein Primideal ersten Grades ist, welches seinem conjugirten gleich wird. Geht die Primzahl 2 in d auf, so wird

$$2 = (2, \sqrt{m})^2, \quad \text{bez.} \quad 2 = (2, 1 + \sqrt{m})^2,$$

je nachdem $m \equiv 2$ oder $\equiv 3$ nach 4 ist.

Die Zerlegung der in d nicht aufgehenden Primzahlen geschieht auf Grund des Satzes 33 unter Berücksichtigung der zu demselben in § 13 S. 202 gemachten Bemerkung. Danach ist eine jede zu d prime rationale Primzahl p im Körper k entweder in zwei von einander verschiedene Primideale zerlegbar oder selbst ein Primideal, je nachdem die linke Seite der in Betracht kommenden Gleichung (21) im Sinne

der Congruenz nach p reducibel oder irreducibel ist. Ist die betreffende Primzahl p ungerade, so finden wir die Congruenz

$$(2x-1)^2-m\equiv 0,\quad \text{bez.}\quad x^2-m\equiv 0,\ (p)$$

offenbar dann reducibel, wenn m quadratischer Rest nach p ist, und dann irreducibel, wenn m quadratischer Nichtrest nach p ist. Setzen wir im ersteren Falle $m\equiv a^2$ nach p, so ergiebt sich:

$$p=(p,\ a+\sqrt{m})(p,\ a-\sqrt{m})=\mathfrak{p}\mathfrak{p}'.$$

Die beiden Primideale $\mathfrak{p}$ und $\mathfrak{p}'$ rechter Hand sind wegen

$$(p,\ a+\sqrt{m},\ a-\sqrt{m})=1$$

in der That von einander verschieden. Im Falle $m\equiv 1$ nach 4 ist die Congruenz $x^2-x-\frac{m-1}{4}\equiv 0$ nach 2 offenbar reducibel oder irreducibel, je nachdem $\frac{m-1}{4}\equiv 0$ oder $\equiv 1$ nach 2 ist, d. h. je nachdem $m\equiv 1$ oder $\equiv 5$ nach 8 ausfällt. Im ersteren Falle findet man:

$$2=\left(2,\ \frac{1+\sqrt{m}}{2}\right)\left(2,\ \frac{1-\sqrt{m}}{2}\right).$$

Die beiden Primideale rechter Hand sind wegen

$$\left(2,\ \frac{1+\sqrt{m}}{2},\ \frac{1-\sqrt{m}}{2}\right)=1$$

in der That von einander verschieden.

Als Basiszahlen der eben aufgestellten Primideale können dienen:

$$\begin{array}{lll} l,\ \dfrac{l+\sqrt{m}}{2}, & \text{bez.} & l,\ \sqrt{m}, \\ p,\ \dfrac{a\pm\sqrt{m}}{2}, & \text{„} & p,\ a\pm\sqrt{m}, \\ 2,\ \dfrac{1\pm\sqrt{m}}{2}, & \text{„} & 2,\ \sqrt{m};\ 2,\ 1+\sqrt{m}, \end{array}$$

je nachdem $m\equiv 1$ oder $\equiv 2, 3$ nach 4 ist. Man erkennt diese Thatsache leicht aus einer Umkehrung des Satzes 19, wenn man jedesmal aus dem hier angegebenen Zahlenpaare und dem dazu conjugirten die Determinante bildet. In der zweiten Zeile der aufgestellten Tabelle soll a eine der Congruenz $a^2\equiv m$ nach p genügende und dazu im Falle $m\equiv 1$ nach 4 ungerade Zahl bedeuten.

§ 61.

Das Symbol $\left(\frac{a}{w}\right)$.

Um die gewonnenen Resultate über die Zerlegung der rationalen Primzahlen in übersichtlicherer Weise aussprechen zu können, führen wir folgendes Symbol ein. Ist a eine beliebige ganze rationale Zahl und w eine ungerade rationale Primzahl, so bedeute **das Symbol** $\left(\frac{a}{w}\right)$ den Wert $+1$, -1 oder 0, je nachdem die Zahl $a \not\equiv 0$ und quadratischer Rest oder quadratischer Nichtrest nach w oder durch w teilbar ist; ferner bedeute $\left(\frac{a}{2}\right)$ den Wert $+1$, -1, oder 0, je nachdem a ungerade und quadratischer Rest oder quadratischer Nichtrest nach $2^3 = 8$ oder durch 2 teilbar ist. Mit Benutzung dieses Symbols erhält der obige Satz 96 folgende Fassung:

Satz 97. Eine beliebige rationale Primzahl p ($= 2$ oder $\neq 2$) ist im Körper k in zwei von einander verschiedene Primideale zerlegbar oder selbst Primideal oder gleich dem Quadrat eines Primideals, je nachdem $\left(\frac{d}{p}\right) = +1$, -1 oder 0 ist. [*Dedekind*[1].]

Wir unterscheiden, den bisherigen Entwickelungen entsprechend, drei Arten von Primidealen, nämlich:

1. die Primideale ersten Grades $\mathfrak{p}$, welche von ihren Conjugirten $\mathfrak{p}'$ verschieden sind;

2. die Primideale zweiten Grades (p), die durch die in k unzerlegbaren rationalen Primzahlen p dargestellt werden;

3. die Primideale ersten Grades $\mathfrak{l}$, deren Quadrate den in d aufgehenden rationalen Primzahlen gleich sind.

Nach den in § 39 und § 41 aufgestellten Definitionen bildet der Körper k für die Primideale $\mathfrak{p}$ der ersten Art den Zerlegungskörper, für die Primideale p der zweiten Art den Trägheitskörper und für die Primideale $\mathfrak{l}$ der dritten Art den Verzweigungskörper.

§ 62.

Die Einheiten des quadratischen Körpers.

Was die Frage nach den Einheiten des Körpers k betrifft, so sind nach Satz 47 die zwei Fälle zu unterscheiden, ob k ein imaginärer oder ein reeller Körper ist.

Im ersteren Falle enthält k nur solche Einheiten, welche zugleich Einheitswurzeln sind, und da in einem quadratischen Körper ausser ± 1 nur die primitiven 3ten, 4ten, 6ten Wurzeln der Einheit vorkommen können, so sind die einzigen imaginären quadratischen Körper, welche noch andere Einheiten als ± 1 enthalten, die zwei Körper $k(\sqrt{-1})$ und $k(\sqrt{-3})$. Der erstere Körper enthält die beiden Einheiten $\pm i$, der letztere die 4 Einheiten $\pm \frac{1 \pm \sqrt{-3}}{2}$. Die Discriminanten dieser zwei Körper sind -4 bez. -3; nach Satz 50 muss daher in jeder Idealklasse dieser Körper ein Ideal vorkommen, dessen Norm $\leqq 2$ bezüglich $\leqq |\sqrt{3}|$ ist. Da ferner im Körper $k(\sqrt{-1})$ die Zahl 2 gleich der Norm des Hauptideals $(1+i)$ wird, so folgt, dass jeder dieser beiden quadratischen Körper nur eine Idealklasse besitzt. Mithin giebt es in diesen Körpern nur Hauptideale, und es ist also jede positive ganze rationale Zahl, welche zur Norm eines Ideals in $k(\sqrt{-1})$ bez. $k(\sqrt{-3})$ geeignet ist, stets Norm einer ganzen algebraischen Zahl in dem betreffenden Körper; hieraus folgen die bekannten Sätze über die Darstellung ganzer rationaler positiver Zahlen in den Gestalten x^2+y^2, bezüglich x^2+xy+y^2, wo x und y ganze rationale Zahlen sein sollen.

Ist dagegen k ein reeller Körper, so giebt es nach Satz 47 stets eine Grundeinheit ε, welche verschieden von ± 1 ist, und durch welche sich jede vorhandene Einheit des Körpers auf eine Weise in der Gestalt $\pm \varepsilon^a$ darstellen lässt, wo a eine ganze rationale Zahl bedeutet.

Die Umstände, unter denen die Norm dieser Grundeinheit ε gleich $+1$ oder gleich -1 ausfällt, sind bisher nur in besonderen Fällen aufgedeckt worden. [*Arndt*[1], *Dirichlet*[4], *Legendre*[1], *Tano*[1].] Vergl. überdies S. 294 den ersten Abschnitt des Beweises zu Hülfssatz 13.

§ 63.

Die Aufstellung des Systems der Idealklassen.

Die Ausführungen in § 24 ermöglichen für jeden besonderen Wert m die Aufstellung aller Idealklassen des quadratischen Körpers k und die Berechnung der Anzahl h dieser Klassen. Hierher gehörige Tabellen sind auf dem Grunde der Theorie der reducirten quadratischen Formen angefertigt worden. [*Gauss*[1], *Cayley*[1].]

Capitel XVII.

Die Geschlechter im quadratischen Körper und ihre Charakterensysteme.

§ 64.

Das Symbol $\left(\frac{n, m}{w}\right)$.

Bei der weiteren Entwickelung der Theorie der quadratischen Körper, insbesondere behufs einer gewissen Einteilung der Idealklassen eines und desselben Körpers, bedienen wir uns eines neuen Symbols. Sind n, m ganze rationale Zahlen, dabei m nicht Quadratzahl, und ist w eine beliebige rationale Primzahl, so bezeichne das **Symbol** $\left(\frac{n, m}{w}\right)$ den Wert $+1$, sobald die Zahl n mit der Norm einer ganzen Zahl des durch $\sqrt{m}$ bestimmten quadratischen Körpers $k(\sqrt{m})$ congruent ist nach der Primzahl w, und sobald ausserdem auch für jede höhere Potenz von w eine ganze Zahl in $k(\sqrt{m})$ existirt, deren Norm der Zahl n nach jener Potenz von w congruent ist; in jedem anderen Falle setzen wir $\left(\frac{n, m}{w}\right) = -1$. Diejenigen ganzen rationalen Zahlen n, für welche $\left(\frac{n, m}{w}\right) = +1$ ist, sollen **Normenreste des Körpers** $k(\sqrt{m})$ **nach** w; diejenigen Zahlen n, für welche $\left(\frac{n, m}{w}\right) = -1$ ist, **Normennichtreste des Körpers** $k(\sqrt{m})$ **nach** w heissen. Ist m eine Quadratzahl, so werde unter $\left(\frac{n, m}{w}\right)$ stets $+1$ verstanden. Ueber die zur Berechnung dienenden Eigenschaften des Symbols $\left(\frac{n, m}{w}\right)$ giebt der folgende Satz Aufschluss:

Satz 98. Bedeuten n und m ganze rationale, nicht durch w teilbare Zahlen, so gelten folgende Regeln:

für ungerade Primzahlen w wird

$$(a') \qquad \left(\frac{n, m}{w}\right) = +1,$$

$$(a'') \qquad \left(\frac{n, w}{w}\right) = \left(\frac{w, n}{w}\right) = \left(\frac{n}{w}\right);$$

für $w = 2$ wird

$$(b') \qquad \left(\frac{n, m}{2}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}},$$

$$(b'') \qquad \left(\frac{n, 2}{2}\right) = \left(\frac{2, n}{2}\right) = (-1)^{\frac{n^2-1}{8}}.$$

Ferner gelten allgemein für beliebige ganze rationale Zahlen n, n', m, m' und in Bezug auf jede Primzahl w die Formeln:

$$(c') \qquad \left(\frac{-m, m}{w}\right) = +1,$$

$$(c'') \qquad \left(\frac{n, m}{w}\right) = \left(\frac{m, n}{w}\right),$$

$$(c''') \qquad \left(\frac{nn', m}{w}\right) = \left(\frac{n, m}{w}\right)\left(\frac{n', m}{w}\right),$$

$$(c'''') \qquad \left(\frac{n, mm'}{w}\right) = \left(\frac{n, m}{w}\right)\left(\frac{n, m'}{w}\right).$$

Beweis. Zunächst ist folgende Thatsache selbstverständlich: Wenn n selbst Norm einer ganzen Zahl im Körper $k(\sqrt{m})$ ist, so gilt $\left(\frac{n, m}{w}\right) = +1$. Da insbesondere $-m$ die Norm von $\sqrt{m}$ ist, so folgt daraus die Richtigkeit der Formel (c'). Sind ferner n und n' zwei ganze rationale Zahlen $\neq 0$, deren Quotient die Norm einer ganzen oder gebrochenen Zahl in $k(\sqrt{m})$ ist, so leuchtet $\left(\frac{n, m}{w}\right) = \left(\frac{n', m}{w}\right)$ aus der Definition dieser Symbole ein. Ist der Quotient $\frac{n}{n'}$ das Quadrat einer rationalen Zahl, so ergiebt sich insbesondere die einfache Thatsache, dass der Wert des Symbols $\left(\frac{n, m}{w}\right)$ ungeändert bleibt, wenn man in n eine Quadratzahl als Factor zusetzt oder einen darin vielleicht vorhandenen solchen Factor unterdrückt. Wir nehmen im Folgenden der Einfachheit halber an, dass weder n noch m durch das Quadrat einer Primzahl teilbar ist.

Um die Richtigkeit des ganzen Formelsystems zu erkennen, behandeln wir der Reihe nach die folgenden drei Fälle:

1) Es sei w eine ungerade, in m aufgehende Primzahl.

Ist n nicht auch durch w teilbar, so wird offenbar die Congruenz

$$(22.) \qquad 4n \equiv (2x+y)^2 - my^2 \quad \text{bez.} \quad n \equiv x^2 - my^2, \ (w),$$

in ganzen rationalen Zahlen x, y dann und nur dann lösbar sein, wenn $\left(\frac{n}{w}\right)=+1$ ist. Umgekehrt, wenn die letztere Bedingung statthat, so ist die Congruenz $n^2 \equiv x^2$ auch nach jeder Potenz von w lösbar, und mithin gilt das nämliche offenbar von der Congruenz (22). Unter den gemachten Annahmen ist daher $\left(\frac{n,m}{w}\right)=\left(\frac{n}{w}\right)$.

Wird andererseits auch n teilbar durch w vorausgesetzt, so folgt:

$$\left(\frac{n,m}{w}\right)=\left(\frac{-nm,m}{w}\right)=\left(\frac{-\frac{nm}{w^2},m}{w}\right)=\left(\frac{-\frac{nm}{w^2}}{w}\right).$$

2) Es sei w eine ungerade, in m nicht aufgehende Primzahl.

Ist auch n nicht durch w teilbar, so hat die Congruenz $n \equiv x^2-my^2$ nach w stets Lösungen. Denn die rechte Seite dieser Congruenz ergiebt für die Systeme $x=1, 2, \ldots, \frac{w-1}{2}$, $y=0$ sämtliche quadratischen Reste und im Falle

$$\left(\frac{-m}{w}\right)=-1$$

für die Systeme $x=0$, $y=1, 2, \ldots, \frac{w-1}{2}$ sämtliche quadratischen Nichtreste nach w. Hat man dagegen $\left(\frac{-m}{w}\right)=+1$, und ist etwa a der kleinste positive quadratische Nichtrest für die Primzahl w, so sei $y=b$ eine Wurzel der alsdann gewiss lösbaren Congruenz $-my^2 \equiv a-1$ nach w; wegen $a \equiv 1-mb^2$ nach w stellt dann die Form $x^2-m(bx)^2$ für $x=1, 2, \ldots, \frac{w-1}{2}$ die sämtlichen quadratischen Nichtreste nach w dar. Aus der Lösbarkeit der Congruenz $n \equiv x^2-my^2$ nach w folgt leicht, dass diese Congruenz auch nach jeder Potenz von w lösbar ist, d. h. es wird unter den gegenwärtigen Annahmen

$$\left(\frac{n,m}{w}\right)=+1.$$

Setzen wir andererseits n durch w teilbar voraus, aber der anfänglichen Festsetzung zufolge nicht teilbar durch w^2, so würde eine Auflösung der Congruenz $n \equiv x^2-my^2$ nach w^2 in $\alpha=x-\sqrt{m}y$ eine solche ganze Zahl des Körpers $k(\sqrt{m})$ darbieten, für welche die

Norm $\alpha . s\alpha = n(\alpha)$ nur w, aber nicht w^2 als Factor enthielte, d. h. w zerfiele im Körper $k(\sqrt{m})$ in zwei von einander verschiedene Primideale $\mathfrak{w}$ und $\mathfrak{w}'$; die notwendige Bedingung hierfür ist nach Satz 97: $\left(\frac{m}{w}\right) = +1$. Umgekehrt, wenn diese Bedingung erfüllt ist, so ist in der That w im Körper $k(\sqrt{m})$ ein Product $\mathfrak{w}\mathfrak{w}'$ zweier verschiedener Primideale. Bezeichnet dann α eine ganze Zahl in $k(\sqrt{m})$, welche durch $\mathfrak{w}$, aber weder durch $\mathfrak{w}^2$ noch durch $\mathfrak{w}'$ teilbar ist, so folgt:

$$\left(\frac{n,\ m}{w}\right) = \left(\frac{n . n(\alpha),\ m}{w}\right) = \left(\frac{\frac{n . n(\alpha)}{w^2},\ m}{w}\right) = +1.$$

Damit ist bewiesen, dass unter der gegenwärtigen Annahme stets $\left(\frac{n,\ m}{w}\right) = \left(\frac{m}{w}\right)$ ist.

Die bisher gewonnenen Resultate lassen unmittelbar die Richtigkeit der Formeln (a'), (a'') erkennen; ferner ergeben sie für ungerade Primzahlen w vollständig die Formeln (c''), (c'''), wenn man der Reihe nach die verschiedenen möglichen Fälle in Hinsicht auf Teilbarkeit oder Nichtteilbarkeit der Zahlen n, n', m durch w in Betracht zieht.

3) Im Falle $w = 2$ stellen wir zunächst folgende Betrachtung an: Es sei $f(x, y)$ eine ganzzahlige homogene Function zweiten Grades von x, y und n eine ungerade ganze rationale Zahl; wenn die Congruenz $n \equiv f(x, y)$ nach 2^3 durch ganze rationale Zahlen x, y lösbar ist, so ist diese Congruenz auch nach jeder höheren Potenz 2^{e+1} ($e \geqq 3$) lösbar. Wir beweisen dies durch einen Schluss von e auf $e+1$. Es seien a, b zwei ganze rationale Zahlen, für welche $n \equiv f(a, b)$ nach 2^e gilt, wobei der Exponent $e \geqq 3$ sei. Ist dann nicht auch zugleich $n \equiv f(a, b)$ nach 2^{e+1}, sondern vielmehr $n \equiv f(a, b) + 2^e$ nach 2^{e+1}, so bestimmen wir, was wegen $e \geqq 3$ angängig ist, eine ganze rationale Zahl c derart, dass $c^2 \equiv 1 + 2^e$ nach 2^{e+1} ist; dann wird

$$\begin{aligned} f(ca,\ cb) = c^2 f(a,\ b) &\equiv f(a,\ b) + 2^e f(a,\ b) \\ &\equiv f(a,\ b) + 2^e \equiv n,\ (2^{e+1}), \end{aligned}$$

und hiermit ist die Behauptung bewiesen.

Um nun zunächst für ein ungerades n das Symbol $\left(\frac{n,\ m}{2}\right)$ zu bestimmen, müssen wir untersuchen, für welche zusammengehörigen

Werte von n und m die Congruenzen

$$(23.)\quad n\equiv x^2+xy-\frac{m-1}{4}y^2, \quad \text{bez.} \quad n\equiv x^2-my^2, \quad (2^3)$$
$$(m\equiv 1, (4)) \qquad\qquad (m\equiv 2, 3, (4))$$

lösbar sind. Eine kurze Rechnung liefert folgende Tabelle, in welcher unter der Rubrik m die sechs hier in Frage kommenden Reste von m nach 2^3 und unter der Rubrik n diejenigen ungeraden Reste von n nach 2^3 verzeichnet stehen, für welche jedesmal die zugehörige Congruenz (23.) nach 2^3 lösbar ist.

m	n	
1	1, 3,	5, 7
2	1, 7	
3	1, 5	
5	1, 3,	5, 7
6	1, 3	
7	1, 5	

Diese Tabelle lehrt für den Fall, dass n, m ungerade sind, die Richtigkeit der Gleichung (b'); und für den Fall, dass n ungerade und m gerade, $=2m'$, ist, entspringt aus ihr:

$$\left(\frac{n,\ 2m'}{2}\right)=(-1)^{\frac{n^2-1}{8}+\frac{n-1}{2}\cdot\frac{m'-1}{2}}.$$

Ist andererseits n gerade, $=2n'$, und m ungerade, so haben wir die beiden Fälle $m\equiv 1$ und $m\equiv 3$ nach 4 zu unterscheiden. Im ersteren Falle muss die Zahl 2 im Körper $k(\sqrt{m})$ jedenfalls das Product zweier verschiedener Primideale sein, sobald $n=2n'$ Normenrest nach 2 in $k(\sqrt{m})$ sein soll, d. h. es muss $\left(\frac{m}{2}\right)=+1$ sein. Ist diese Bedingung erfüllt, so kann man stets in $k(\sqrt{m})$ eine Zahl α finden, für welche die Norm $n(\alpha)$ durch 2, aber nicht durch 4 teilbar ist; dann folgt:

$$\left(\frac{2n', m}{2}\right) = \left(\frac{2n'.n(\alpha), m}{2}\right) = \left(\frac{\frac{n'.n(\alpha)}{2}, m}{2}\right),$$

und dieses letztere Symbol ist nach Formel (b') gleich $+1$; mithin gilt in diesem Falle die Formel:

$$\left(\frac{2n', m}{2}\right) = \left(\frac{m}{2}\right) = (-1)^{\frac{m^2-1}{8}}.$$

In dem anderen Falle, $m \equiv 3$ nach 4, hängt der Wert des fraglichen Symbols von der Lösbarkeit der Congruenz $2n' \equiv x^2 - my^2$ nach beliebig hohen Potenzen 2^e ab, und jede solche Congruenz ist, wie man leicht sieht, dann und nur dann lösbar, wenn die Congruenz $m \equiv x^2 - 2n'y^2$ nach der nämlichen Potenz 2^e lösbar ist; also findet man hier:

$$\left(\frac{2n', m}{2}\right) = \left(\frac{m, 2n'}{2}\right).$$

Sind endlich die Zahlen n und m beide durch 2 teilbar, und ist $n = 2n'$ und $m = 2m'$, so gilt die Formel:

$$\left(\frac{2n', 2m'}{2}\right) = \left(\frac{-2^2n'm', 2m'}{2}\right) = \left(\frac{-n'm', 2m'}{2}\right).$$

Aus den gewonnenen Resultaten folgt unmittelbar die Formel (b''); zugleich erkennen wir, dass die Formeln (c''), (c''') auch für $w = 2$ gültig sind. Die Formel (c'''') folgt allgemein durch Verbindung von (c''') mit (c''). Damit ist der Beweis des Satzes 98 in allen Teilen erbracht.

§ 65.

Das Charakterensystem eines Ideals.

Wir bezeichnen die verschiedenen in der Discriminante des Körpers $k(\sqrt{m})$ aufgehenden rationalen Primzahlen, deren Anzahl t sei, mit $l_1, \ldots, l_t$. Zu einer jeden beliebigen ganzen rationalen Zahl a gehören dann ganz bestimmte Werte ($= +1$ oder -1) der t einzelnen Symbole

$$\left(\frac{a, m}{l_1}\right), \quad \ldots, \quad \left(\frac{a, m}{l_t}\right),$$

deren Bedeutung aus dem vorigen Paragraphen zu ersehen ist; diese t Einheiten ± 1 sollen **das Charakterensystem der Zahl** a im

Körper $k(\sqrt{m})$ heissen. Um auch einem jeden Ideal $\mathfrak{a}$ des Körpers $k(\sqrt{m})$ in bestimmter Weise ein Charakterensystem zuzuordnen, unterscheiden wir die zwei Fälle, ob k ein imaginärer oder ein reeller Körper ist. Im ersteren Falle sind die Normen von Zahlen in $k(\sqrt{m})$ stets positiv; wir setzen $r = t$, $\bar{n} = +n(\mathfrak{a})$ und bezeichnen die r Einheiten

$$(24.)\qquad \left(\frac{\bar{n}, m}{l_1}\right), \quad \ldots, \quad \left(\frac{\bar{n}, m}{l_r}\right)$$

als das **Charakterensystem des Ideals** $\mathfrak{a}$; dasselbe ist durch das Ideal $\mathfrak{a}$ völlig eindeutig bestimmt. Im zweiten Falle bilden wir zunächst das Charakterensystem der Zahl -1:

$$(25.)\qquad \left(\frac{-1, m}{l_1}\right), \quad \ldots, \quad \left(\frac{-1, m}{l_t}\right).$$

Fallen diese t Einheiten sämtlich gleich $+1$ aus, so setzen wir wie im ersteren Falle $\bar{n} = +n(\mathfrak{a})$, $r = t$ und bezeichnen wieder die r Einheiten (24.) als das **Charakterensystem des Ideals** $\mathfrak{a}$. Kommt dagegen unter den t Charakteren (25.) die Einheit -1 vor, so nehmen wir an, es sei etwa $\left(\frac{-1, m}{l_t}\right) = -1$, und setzen $r = t-1$ und $\bar{n} = \pm n(\mathfrak{a})$ mit solchem Vorzeichen $\pm$, dass $\left(\frac{\bar{n}, m}{l_t}\right) = +1$ wird, und nennen die bei dieser Annahme von r und $\bar{n}$ entspringenden r Einheiten (24.) das **Charakterensystem des Ideals** $\mathfrak{a}$. Bei den so getroffenen Festsetzungen wird der folgende Satz 99 sich ergeben.

§ 66.

Das Charakterensystem einer Idealklasse und der Begriff des Geschlechts.

Satz 99. Die Ideale einer und derselben Klasse im Körper $k(\sqrt{m})$ besitzen alle dasselbe Charakterensystem.

Beweis. Gehören die Ideale $\mathfrak{a}$ und $\mathfrak{a}'$ in $k(\sqrt{m})$ zu einer und derselben Idealklasse, so existirt eine ganze oder gebrochene Zahl α in $k(\sqrt{m})$ von der Art, dass $\mathfrak{a}' = \alpha\mathfrak{a}$ wird. Alsdann ist $n(\mathfrak{a}') = \pm n(\alpha) n(\mathfrak{a})$, wo $\pm$ das Vorzeichen von $n(\alpha)$ bedeutet, und es wird daher:

$$\left(\frac{n(\mathfrak{a}'), m}{l}\right) = \left(\frac{\pm n(\mathfrak{a}), m}{l}\right)$$

für $l = l_1, \ldots, l_t$. Mit Rücksicht auf die Festsetzungen in § 65 erhält man sogleich den Satz 99.

Auf diese Weise ist einer jeden Idealklasse ein bestimmtes Charakterensystem zugeordnet. Wir rechnen nun alle diejenigen Idealklassen, welche ein und dasselbe Charakterensystem besitzen, in ein **Geschlecht** und definiren insbesondere das **Hauptgeschlecht** als die Gesamtheit aller derjenigen Klassen, deren Charakterensystem aus lauter positiven Einheiten besteht. Da das Charakterensystem der Hauptklasse offenbar von der letzteren Eigenschaft ist, so gehört die Hauptklasse stets zum Hauptgeschlecht. Aus der Formel (c'') auf S. 287 entnehmen wir leicht die Thatsache, dass die Multiplication der Idealklassen zweier Geschlechter die Idealklassen eines Geschlechtes liefert, dessen Charakterensystem durch Multiplication der entsprechenden Charaktere beider Geschlechter erhalten wird. Im Besonderen folgt, dass das Charakterensystem des Quadrates einer Idealklasse aus einem ganz beliebigen Geschlecht stets aus lauter positiven Einheiten besteht und mithin das Quadrat einer jeden Idealklasse stets dem Hauptgeschlecht angehört.

Jedes Geschlecht enthält offenbar gleich viel Klassen.

§ 67.

Der Fundamentalsatz über die Geschlechter des quadratischen Körpers.

Es entsteht nun die Frage, ob ein jedes beliebige System von r Einheiten ± 1 das Charakterensystem eines Geschlechtes des Körpers $k(\sqrt{m})$ sein kann. Die Beantwortung dieser Frage ist für die Theorie der quadratischen Körper von grundlegender Bedeutung; sie ist in folgendem Satz enthalten, dessen Beweis uns bis zum § 78 beschäftigen wird:

Satz 100. *Ein beliebig vorgelegtes System von r Einheiten ± 1 ist dann und nur dann Charakterensystem eines Geschlechtes des Körpers $k(\sqrt{m})$, wenn das Product der sämtlichen r Einheiten $= +1$ ist. Die Anzahl der im Körper $k(\sqrt{m})$ vorhandenen Geschlechter ist daher gleich 2^{r-1}.* [*Gauss*[1].]

§ 68.

Ein Hülfssatz über diejenigen quadratischen Körper, deren Discriminanten nur durch eine einzige Primzahl teilbar sind.

Um uns dem durch den Satz 100 gesteckten Ziele zu nähern, beweisen wir zunächst folgenden Hülfssatz:

Hülfssatz 13. Wenn in der Discriminante eines quadratischen Körpers

$k = k(\sqrt{m})$ nur eine einzige rationale Primzahl l aufgeht, so ist die Anzahl der Idealklassen in k ungerade. Das Charakterensystem besteht für den Körper k aus dem einen, auf die Primzahl l bezüglichen Charakter; dieser Charakter ist stets $= +1$, d. h. es giebt im Körper k nur ein Geschlecht: das Hauptgeschlecht.

Beweis. Wir bezeichnen mit s diejenige Substitution für die Zahlen des Körpers k, welche aus ihnen die Conjugirten entstehen lässt. Es bedeute im Falle $m > 0$ wieder ε eine Grundeinheit des Körpers k, eine ebensolche Einheit stellen $-\varepsilon$, $\frac{1}{\varepsilon}$, $-\frac{1}{\varepsilon}$ vor; wir beweisen dann zunächst, dass bei der im Hülfssatze gemachten Voraussetzung notwendig $n(\varepsilon) = \varepsilon . s\varepsilon = -1$ ausfallen muss. In der That, nehmen wir an, es wäre $n(\varepsilon) = +1$, so könnte man nach Satz 90 eine ganze Zahl α des Körpers k finden derart, dass man $\varepsilon = \frac{\alpha}{s\alpha}$ hätte; dann folgt $\alpha = \varepsilon . s\alpha$, d. h. jeder in α aufgehende ideale Primfactor ginge auch in $s\alpha$ auf. Da für $m > 0$ unter der im Hülfssatze gemachten Voraussetzung $\sqrt{m}$ der einzige, seinem conjugirten gleiche und nicht zugleich rationale Primfactor in k ist, so muss entweder $\alpha = \eta a$ oder $= \eta\sqrt{m}\, a$ sein, wo η eine Einheit und a eine ganze rationale positive oder negative Zahl bedeutet; hieraus würde $\varepsilon = \pm\eta^{1-s} = \pm\eta^2$ hervorgehen, und dies widerspräche der Annahme, dass ε eine Grundeinheit des Körpers k ist.

Nunmehr gehen wir dazu über, den ersten Teil des Hülfssatzes zu beweisen. Wäre für den Körper k die Klassenanzahl h eine gerade Zahl, so müsste es nach Satz 57 in k ein nicht zur Hauptklasse gehöriges Ideal $\mathfrak{j}$ geben derart, dass $\mathfrak{j}^2 \sim 1$ ist; wegen $\mathfrak{j} . s\mathfrak{j} \sim 1$ würde hieraus $\mathfrak{j} \sim s\mathfrak{j}$ folgen. Setzen wir $\mathfrak{j} = \alpha . s\mathfrak{j}$ oder $\mathfrak{j}^{1-s} = \alpha$, so ist α eine Zahl in k, deren Norm $n(\alpha) = \pm 1$ sein muss. Im Falle, dass hier das positive Vorzeichen statthätte, setze man $\beta = \alpha$; der andere Fall ist von vornherein nur bei einem reellen Körper denkbar; wir setzen dann $\beta = \varepsilon\alpha$, wo ε, wie vorhin, die Grundeinheit in k bedeutet. Unter den getroffenen Festsetzungen hätte man jedesmal $n(\beta) = +1$, und mithin wäre nach Satz 90 stets $\frac{1}{\beta} = \gamma^{1-s}$, wo γ eine ganze Zahl in k bezeichnet. Aus $\alpha = \mathfrak{j}^{1-s}$ entstünde dann $(\gamma\mathfrak{j})^{1-s} = 1$, d. h. $(\gamma)\mathfrak{j} = s(\gamma\mathfrak{j})$, und hieraus würde, ähnlich wie vorhin, folgen, dass das Ideal $(\gamma)\mathfrak{j}$ entweder $= (a)$ oder $= (a)\mathfrak{l}$ sein muss, wo a eine ganze rationale Zahl und $\mathfrak{l}$ den einzigen in k vorhandenen, seinem Conjugirten gleichen und nicht zugleich

rationalen Primfactor bezeichnet. Nun ist für $m \neq -1$ dieser Primfactor $\mathfrak{l} = \sqrt{m}$ und für $m = -1$ offenbar $\mathfrak{l} = 1 + \sqrt{-1}$, also stets $\mathfrak{l} \sim 1$; somit würde $\mathfrak{j} \sim 1$ folgen, was der über $\mathfrak{j}$ gemachten Annahme zuwiderläuft.

Ist k ein reeller Körper, so folgt zugleich aus $n(\varepsilon) = -1$, dass

$$\left(\frac{-1, m}{l}\right) = +1$$

ist, und es besteht mithin gemäss § 65 in jedem Falle das Charakterensystem für ein Ideal $\mathfrak{j}$ im Körper k aus der einen Einheit $\left(\frac{+n(\mathfrak{j}), m}{l}\right)$; dieser eine Charakter ist für jedes Ideal $\mathfrak{j}$ in k gleich $+1$, da sonst die Gesamtheit der Idealklassen von k in zwei Geschlechter zerfiele und somit die Klassenanzahl h gerade sein müsste.

Der eben bewiesene Hülfssatz 13 zeigt die Richtigkeit des Fundamentalsatzes 100 im einfachsten Falle, nämlich für diejenigen quadratischen Körper, deren Discriminante d nur eine einzige rationale Primzahl enthält.

§ 69.

Das Reciprocitätsgesetz für quadratische Reste. Ein Hülfssatz über das Symbol $\left(\frac{n, m}{w}\right)$.

Satz 101. *Sind p, q rationale positive, von einander verschiedene, ungerade Primzahlen, so gilt die Regel:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

das sogenannte Reciprocitätsgesetz für quadratische Reste. Ueberdies gelten die folgenden Regeln:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

die sogenannten Ergänzungssätze zum quadratischen Reciprocitätsgesetz. [*Gauss*[1].]

Beweis. Ist $k(\sqrt{m})$ ein Körper, dessen Discriminante nur eine Primzahl l enthält, und bedeutet n die Norm eines Ideals in diesem Körper k, so ist nach dem Hülfssatze 13 stets $\left(\frac{n, m}{l}\right) = +1$. Nun ist nach Satz 96 oder 97 insbesondere jede positive ungerade und in m nicht aufgehende rationale Primzahl, von welcher m quadratischer Rest ist, Norm

eines Ideals in $k(\sqrt{m})$. Die Benutzung dieses Umstandes liefert uns die nachstehende Tabelle; in derselben bedeuten p, p' irgend von einander verschiedene positive rationale und der Zahl 1 nach 4 congruente Primzahlen, und andererseits bedeuten q, q' von einander verschiedene positive rationale und der Zahl 3 nach 4 congruente Primzahlen, während r eine positive rationale ungerade Primzahl bezeichnet, von welcher kein bestimmter Restcharakter nach 4 vorausgesetzt wird.

	Wenn:				so ist:
	m	l	n	$\left(\frac{m}{n}\right)=+1$	$\left(\frac{n,m}{l}\right)=+1$
1.	-1	2	r	$\left(\frac{-1}{r}\right)=+1$	$\left(\frac{r,-1}{2}\right)=(-1)^{\frac{r-1}{2}}=+1$
2.	2	2	r	$\left(\frac{2}{r}\right)=+1$	$\left(\frac{r,2}{2}\right)=(-1)^{\frac{r^2-1}{8}}=+1$
3.	p	p	p'	$\left(\frac{p}{p'}\right)=+1$	$\left(\frac{p',p}{p}\right)=\left(\frac{p'}{p}\right)=+1$
4.	p	p	q	$\left(\frac{p}{q}\right)=+1$	$\left(\frac{q,p}{p}\right)=\left(\frac{q}{p}\right)=+1$
5.	$-q$	q	p	$\left(\frac{-q}{p}\right)=+1$	$\left(\frac{p,-q}{q}\right)=\left(\frac{p}{q}\right)=+1$
6.	$-q$	q	q'	$\left(\frac{-q}{q'}\right)=+1$	$\left(\frac{q',-q}{q}\right)=\left(\frac{q'}{q}\right)=+1$

Nehmen wir die in einem Körper $k(\sqrt{p})$ aus $n(\varepsilon)=-1$ folgende Thatsache, dass $\left(\frac{-1}{p}\right)=+1$ ist, zur Zeile 1 dieser Tabelle hinzu, so folgt allgemein $\left(\frac{-1}{r}\right)=(-1)^{\frac{r-1}{2}}$. Wenden wir ferner die am Eingange dieses Beweises genannte Thatsache auf die Primzahl $n=2$ an, und berücksichtigen wir, dass die Zahl 2 stets gleich der Norm eines Ideals in $k(\sqrt{p})$ oder in $k(\sqrt{-q})$ ist, sobald $(-1)^{\frac{p^2-1}{8}}=+1$, bezüglich $(-1)^{\frac{q^2-1}{8}}=+1$ statthat, so folgt, dass unter der letzteren Voraussetzung stets $\left(\frac{2,p}{p}\right)=\left(\frac{2}{p}\right)=+1$, bezüglich $\left(\frac{2,-q}{q}\right)=\left(\frac{2}{q}\right)=+1$ ist,

d. h.: wenn $(-1)^{\frac{r^2-1}{8}} = +1$ ist, so ist $\left(\frac{2}{r}\right) = +1$. Nehmen wir diese Thatsache zur Zeile 2 der obigen Tabelle hinzu, so folgt allgemein $\left(\frac{2}{r}\right) = (-1)^{\frac{r^2-1}{8}}$. Aus dem Inhalte der Zeile 3 folgt $\left(\frac{p}{p'}\right) = \left(\frac{p'}{p}\right)$. Aus Zeile 4 und 5 folgt $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, und Zeile 6 ergiebt:

$$\left(\frac{q}{q'}\right) = -\left(\frac{q'}{q}\right);$$

dabei ist noch jedesmal der Restcharakter von -1 in Rücksicht zu ziehen, welcher oben gefunden worden ist.

Hülfssatz 14. Wenn n und m zwei beliebige ganze rationale Zahlen bedeuten, welche nicht beide negativ sind, so ist

$$\underset{(w)}{\Pi}\left(\frac{n, m}{w}\right) = +1,$$

wo das Product linker Hand über sämtliche rationale Primzahlen w zu erstrecken ist.

Beweis. Bedeuten p, q beliebige rationale ungerade, von einander verschiedene Primzahlen, so folgen aus den Regeln (a''), (b'), (b'') in § 64 und aus Satz 101 leicht die Formeln:

$$\left(\frac{-1, 2}{2}\right) = +1, \quad \left(\frac{-1, p}{2}\right)\left(\frac{-1, p}{p}\right) = +1,$$

$$\left(\frac{2, 2}{2}\right) = +1, \quad \left(\frac{2, p}{2}\right)\left(\frac{2, p}{p}\right) = +1,$$

$$\left(\frac{p, p}{2}\right)\left(\frac{p, p}{p}\right) = +1, \quad \left(\frac{p, q}{2}\right)\left(\frac{p, q}{p}\right)\left(\frac{p, q}{q}\right) = +1;$$

mit Rücksicht auf die Regel (a') in § 64 besteht danach der Hülfssatz 14 für den Fall, dass die Zahlen n, m gleich ± 1 sind oder nur einen Primzahlfactor enthalten. Wegen der Formeln (c'''), (c'''') in § 64 gilt demnach der Hülfssatz 14 allgemein.

Zugleich folgt wegen $\left(\frac{-1, -1}{2}\right) = -1$, dass, wenn die Zahlen n und m beide negativ angenommen werden, das entsprechende Product $\underset{(w)}{\Pi}$ den Wert -1 hat. Die im Hülfssatze 14 ausgesprochene und diese weitere Behauptung erhalten, wie man leicht erkennt, einen ein-

heitlichen Ausdruck, wenn man sich des neuen Symbols $\left(\frac{n, m}{-1}\right) = \pm 1$ bedienen will, wo rechter Hand das positive oder das negative Vorzeichen gelten soll, je nachdem wenigstens eine der beiden Zahlen n, m positiv ist oder beide negativ ausfallen.

§ 70.

Beweis der im Fundamentalsatz 100 ausgesprochenen Beziehung zwischen den sämtlichen Charakteren eines Geschlechts.

Der im § 69 bewiesene Hülfssatz 14 dient dazu, um den einen Teil unseres Fundamentalsatzes 100 zu beweisen. Bedeutet A irgend eine Idealklasse des Körpers $k(\sqrt{m})$, ist dann $\mathfrak{a}$ ein zu 2 und zu d primes Ideal der Klasse A, und wird $\bar{n} = \pm n(\mathfrak{a})$ die mit dem betreffenden Vorzeichen gemäss § 65 versehene Norm des Ideals $\mathfrak{a}$, so ist das Product der sämtlichen Charaktere der Klasse A durch den Ausdruck:

$$\left(\frac{\bar{n}, m}{l_1}\right) \cdots \left(\frac{\bar{n}, m}{l_r}\right)$$

gegeben. Da $n(\mathfrak{a})$ die Norm eines Ideals ist, so muss eine jede in $\bar{n}$ zu ungerader Potenz vorkommende rationale Primzahl p im Körper $k(\sqrt{m})$ zerlegbar sein; es ist mithin nach Satz 96 m von jeder solchen Primzahl p quadratischer Rest. Aus Hülfssatz 14 und unter Heranziehung der Formeln (c'''), (a'), (a'') aus Satz 98 folgt daher:

$$\prod_{(w)} \left(\frac{\bar{n}, m}{w}\right) = +1,$$

wenn w alle in m enthaltenen ungeraden Primzahlen und die Primzahl 2 durchläuft.

Kommt nun in der Discriminante d des Körpers $k(\sqrt{m})$ die Primzahl 2 vor, so ist schon hiermit bewiesen, dass für jede Klasse in $k(\sqrt{m})$ das Product sämtlicher Charaktere $= +1$ ist.

Kommt dagegen die Primzahl 2 in d nicht vor, so hat man, wegen $m \equiv 1$ nach 4, stets $\left(\frac{\bar{n}, m}{2}\right) = +1$, und damit ist auch in diesem Falle der gewünschte Nachweis erbracht.

Durch den soeben geführten Nachweis, dass das Product aller Charaktere $= +1$ ist, erkennen wir zugleich, dass die Anzahl der Geschlechter im quadratischen Körper $k(\sqrt{m})$ höchstens gleich der Hälfte aller an sich denkbaren Charakterensysteme, d. h. höchstens gleich 2^{r-1} sein kann.

Capitel XVIII.

Die Existenz der Geschlechter im quadratischen Körper.

§ 71.

Der Satz von den Normen der Zahlen eines quadratischen Körpers.

Es bleibt noch übrig, den anderen Teil des Fundamentalsatzes 100 als richtig zu erkennen, d. h. den Nachweis zu führen, dass die eben gefundene Bedingung, welche ein System von r Einheiten ± 1 notwendig erfüllen muss, damit dasselbe als das Charakterensystem eines Geschlechtes in $k(\sqrt{m})$ vorkommen kann, auch für diesen Umstand hinreichend ist. Dieser Nachweis kann auf zwei völlig verschiedenen Wegen erbracht werden; der erste Weg ist rein arithmetischer Natur, der zweite benutzt wesentlich transcendente Hülfsmittel. Der erste Beweis geschieht durch folgende Ueberlegungen:

Satz 102. Wenn n, m zwei ganze rationale Zahlen bedeuten, von denen m keine Quadratzahl ist, und die für jede beliebige Primzahl w die Bedingung

$$\left(\frac{n, m}{w}\right) = +1$$

erfüllen, so ist die Zahl n stets gleich der Norm einer ganzen oder gebrochenen Zahl α des Körpers $k(\sqrt{m})$.

Beweis. Wegen $\prod_{(w)} \left(\frac{n, m}{w}\right) = +1$ ist gemäss der Bemerkung auf S. 297 unten wenigstens eine der beiden Zahlen n, m negativ. Wir dürfen voraussetzen, dass n und m keine rationalen quadratischen Factoren enthalten. Bedeutet dann p eine in n als Factor enthaltene Primzahl, welche zugleich in der Discriminante d des Körpers $k(\sqrt{m})$ aufgeht, so ist p gleich der Norm eines Ideals in $k(\sqrt{m})$. Bedeutet ferner p eine ungerade, in n, aber nicht in m aufgehende Primzahl, so ist, wegen

$$\left(\frac{n, m}{p}\right) = \left(\frac{m}{p}\right) = +1,$$

diese Primzahl p ebenfalls gleich der Norm eines Ideals in $k(\sqrt{m})$. Ist endlich die Primzahl 2 in n, aber nicht in der Discriminante des Körpers $k(\sqrt{m})$ enthalten, so ist wegen $\left(\frac{n, m}{2}\right) = \left(\frac{2, m}{2}\right) = (-1)^{\frac{m^2-1}{8}} = +1$

wiederum die Primzahl 2 gleich der Norm eines Ideals in $k(\sqrt{m})$, und mithin giebt es in $k(\sqrt{m})$ gewiss stets ein Ideal $\mathfrak{j}$ derart, dass $|n| = n(\mathfrak{j})$ wird. Wir wählen nun in der durch $\mathfrak{j}$ bestimmten Idealklasse ein solches Ideal $\mathfrak{j}'$ aus, dessen Norm $n(\mathfrak{j}') \leqq |\sqrt{d}|$ ist, wo d die Discriminante des durch $\sqrt{m}$ bestimmten Körpers bedeutet. Dies ist nach Satz 50 stets möglich. Wir setzen dann $\mathfrak{j}' = \varkappa \mathfrak{j}$ und $n' = n.n(\varkappa)$; dabei bedeutet $\varkappa$ eine ganze oder gebrochene Zahl in $k(\sqrt{m})$, und es wird $n' = \pm n(\mathfrak{j}')$, wo das positive oder das negative Vorzeichen gilt, je nachdem $n.n(\varkappa)$ positiv oder negativ ausfällt. Die ganze rationale Zahl n' fällt daher insbesondere gewiss positiv aus, falls m negativ ist. Da d den Wert m oder $4m$ hat, so ist gewiss $|n'| \leqq 2|\sqrt{m}|$, und hieraus folgt $|n'| < |m|$, sobald $2|\sqrt{m}| < |m|$, d. h. $|m| > 4$ ist. Andererseits gilt wegen $n' = n.n(\varkappa)$ die Gleichung $\left(\frac{n, m}{w}\right) = \left(\frac{n', m}{w}\right) = +1$ und dann nach Formel (c'') in Satz 98 auch $\left(\frac{m, n'}{w}\right) = +1$ für jede beliebige Primzahl w.

Wir machen nun die Annahme, dass der zu beweisende Satz 102 bereits für jeden Körper $k(\sqrt{m'})$ feststehe, bei welchem die bestimmende Zahl m', mag sie positiv oder negativ sein, der Ungleichung $|m'| < |m|$ genügt. Sowie die vorhin gefundene Zahl n' die Bedingung $|n'| < |m|$ erfüllt und keine Quadratzahl ist, muss dann, da auch die Bedingung $\left(\frac{m, n'}{w}\right) = +1$ für jede beliebige Primzahl w gilt, infolge der angenommenen Gültigkeit unseres Satzes 102, die Zahl m die Norm einer Zahl α' im Körper $k(\sqrt{n'})$ sein, d. h. es gibt zwei ganze oder gebrochene rationale Zahlen a und b derart, dass $m = a^2 - n'b^2$ wird; wenn aber n' eine Quadratzahl ist, so versteht sich die Möglichkeit dieser Gleichung ohne weiteres. Da $b \neq 0$ sein muss, so folgt hieraus $n' = \left(\frac{a}{b}\right)^2 - m\left(\frac{1}{b}\right)^2 = n(\lambda)$, d. h. es ist n' die Norm einer Zahl λ im Körper $k(\sqrt{m})$. Die Verbindung dieser Thatsache mit der Gleichung $n' = n.n(\varkappa)$ ergiebt $n = n(\alpha)$, wo $\alpha = \frac{\lambda}{\varkappa}$ wieder eine Zahl in $k(\sqrt{m})$ bedeutet.

Der vollständige Beweis unseres Satzes 102 wird hiernach offenbar geführt sein, sobald wir seine Richtigkeit für alle die Fälle erkannt haben, in denen $|m| \leqq 4$ und zugleich $|n| \leqq |\sqrt{d}|$ statthat. Bei dieser Einschränkung der Zahlen n, m treffen die Bedingungen des Satzes 102 nur in 8 Fällen zu. Die Gleichungen

$$1 = n(\sqrt{-1}), \qquad -2 = n(\sqrt{2}),$$
$$2 = n(1+\sqrt{-1}), \qquad 2 = n(\sqrt{-2}),$$
$$2 = n(2+\sqrt{2}), \qquad -2 = n(1+\sqrt{3}),$$
$$-1 = n(1+\sqrt{2}), \qquad -3 = n(\sqrt{3}),$$

zeigen, dass in diesen 8 Fällen unser Satz 102 gültig ist.

Man erkennt leicht, dass der Satz 102 auch in der Abänderung zutrifft, dass die Erfüllung der Bedingung $\left(\frac{n, m}{w}\right) = +1$ nur für alle ungeraden Primzahlen w verlangt, dann aber die Bedingung hinzugefügt wird, dass wenigstens eine der beiden Zahlen n, m negativ ist [*Lagrange*[1], *Legendre*[1], *Gauss*[1]]; in der That ist nach Hülfssatz 14 die Gleichung $\left(\frac{n, m}{2}\right) = +1$ dann von selbst miterfüllt.

§ 72.

Die Klassen des Hauptgeschlechtes.

Am Schlusse des § 66 haben wir gezeigt, dass das Quadrat einer Idealklasse stets dem Hauptgeschlechte angehört. Durch den Satz 102 des § 71 haben wir ein Mittel, die umgekehrte Thatsache einzusehen.

Satz 103. In einem quadratischen Körper ist jede Klasse des Hauptgeschlechtes stets gleich dem Quadrat einer Klasse. [*Gauss*[1].]

Beweis. Es sei H im Körper $k(\sqrt{m})$ eine Klasse des Hauptgeschlechts, $\mathfrak{h}$ ein solches Ideal aus der Klasse H, welches zur Discriminante d des Körpers $k(\sqrt{m})$ prim ausfällt, und $\bar{n}$ sei die mit dem bezüglichen Vorzeichen gemäss § 65 versehene Norm des Ideals $\mathfrak{h}$. Diese Zahl $\bar{n}$ erfüllt dann für jede beliebige Primzahl w die Bedingung $\left(\frac{\bar{n}, m}{w}\right) = +1$, und es ist mithin dem Satze 102 zufolge $\bar{n} = n(\alpha)$, wo α eine ganze oder gebrochene Zahl des Körpers $k(\sqrt{m})$ bedeutet. Setzen wir $\frac{\mathfrak{h}}{\alpha} = \frac{\mathfrak{k}}{\mathfrak{k}'}$, wo $\mathfrak{k}$ und $\mathfrak{k}'$ zu einander prime Ideale seien, so folgt $\frac{\mathfrak{k}.s\mathfrak{k}}{\mathfrak{k}'.s\mathfrak{k}'} = 1$, und mithin ist notwendigerweise $\mathfrak{k}' = s\mathfrak{k}$. Da $\mathfrak{k}.s\mathfrak{k} \sim 1$ ist, so folgt $\mathfrak{h} \sim \mathfrak{k}^2$.

Die eben bewiesene charakteristische Eigenschaft der Ideale des Hauptgeschlechts steht in engem Zusammenhange mit einer anderen gleichfalls charakteristischen Eigenschaft dieser Ideale, welche in folgendem Satze ihren Ausdruck findet:

Satz 104. Sind ω_1, ω_2 Basiszahlen des quadratischen Körpers k und η_1, η_2 Basiszahlen eines zum Hauptgeschlecht von k gehörigen Ideals $\mathfrak{h}$, und ist endlich N eine beliebig gegebene ganze rationale Zahl, so lassen sich stets vier rationale Zahlen r_{11}, r_{12}, r_{21}, r_{22} finden, deren Nenner zu N prim sind, für welche die Determinante $r_{11}r_{22}-r_{12}r_{21}$ den Wert ± 1 hat, und vermittelst derer

$$\frac{\eta_1}{\eta_2}=\frac{r_{11}\omega_1+r_{12}\omega_2}{r_{21}\omega_1+r_{22}\omega_2}$$

wird.

Beweis. Man bestimme ein zu $\mathfrak{h}$ äquivalentes Ideal $\mathfrak{h}'=\beta\mathfrak{h}$, welches zu Nd prim ist. Wie in dem Beweise zum Satz 103 bereits benutzt wurde, ist $\bar{n}=\pm n(\mathfrak{h}')$, wenn das Vorzeichen gemäss § 65 gewählt wird, stets gleich der Norm einer ganzen oder gebrochenen Zahl α im Körper k. Das Ideal $\alpha\mathfrak{h}'=\alpha\beta\mathfrak{h}$ besitzt die Basiszahlen

$$\begin{aligned}\alpha\beta\eta_1 &= a_{11}\omega_1+a_{12}\omega_2,\\ \alpha\beta\eta_2 &= a_{21}\omega_2+a_{22}\omega_2,\end{aligned}$$

wo a_{11}, a_{12}, a_{21}, a_{22} ganze rationale Zahlen bedeuten. Wegen $n(\alpha\mathfrak{h}')=\bar{n}^2$ ist die Determinante $a_{11}a_{22}-a_{12}a_{21}=\pm\bar{n}^2$, und daher besitzen die vier Zahlen $r_{11}=\frac{a_{11}}{\bar{n}}$, $r_{12}=\frac{a_{12}}{\bar{n}}$, $r_{21}=\frac{a_{21}}{\bar{n}}$, $r_{22}=\frac{a_{22}}{\bar{n}}$ die im Satze behaupteten Eigenschaften.

§ 73.
Die ambigen Ideale.

Im quadratischen Körper k werde ein Ideal $\mathfrak{a}$ ein **ambiges Ideal** genannt, wenn es nach Anwendung der Operation $s=(\sqrt{m}:-\sqrt{m})$ ungeändert bleibt, und wenn es ausserdem keine ganze rationale Zahl $\neq\pm 1$ als Factor enthält. (Vgl. § 57.) Es gilt die Thatsache:

Satz 105. Die t in der Discriminante d des Körpers k aufgehenden, von einander verschiedenen Primideale $\mathfrak{l}_1,\ldots,\mathfrak{l}_t$, und nur diese, sind ambige Primideale in k. Die 2^t Ideale $1,\mathfrak{l}_1,\mathfrak{l}_2,\ldots,\mathfrak{l}_1\mathfrak{l}_2,\ldots,\mathfrak{l}_1\mathfrak{l}_2\ldots\mathfrak{l}_t$ machen die Gesamtheit aller ambigen Ideale des Körpers k aus.

Beweis. Dass die Primideale $\mathfrak{l}_1,\ldots,\mathfrak{l}_t$, und nur diese, ambig sind, folgt aus Satz 96. Ist nun $\mathfrak{a}=\mathfrak{p}\mathfrak{q}\ldots\mathfrak{r}$ ein beliebiges, in Primideale zerlegtes ambiges Ideal, so müssen wegen $\mathfrak{a}=s\mathfrak{a}$ die zu den Primidealen

$\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{r}$ conjugirten Primideale $s\mathfrak{p}, s\mathfrak{q}, \ldots, s\mathfrak{r}$, von der Reihenfolge abgesehen, mit $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{r}$ übereinstimmen. Wenn etwa $s\mathfrak{p} = \mathfrak{q}$ sich herausstellen würde, so besässe $\mathfrak{a}$ den Factor $\mathfrak{p}.s\mathfrak{p}$, welcher gleich einer ganzen rationalen Zahl ist; da dieser Umstand der Erklärung des ambigen Ideals zuwider wäre, so muss notwendig $\mathfrak{p} = s\mathfrak{p}$ sein und ebenso $\mathfrak{q} = s\mathfrak{q}, \ldots, \mathfrak{r} = s\mathfrak{r}$, d. h. die einzelnen Primideale $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{r}$ sind sämtlich ambig. Da die Quadrate der Ideale $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$ gleich ganzen rationalen Zahlen werden, so schliessen wir ebenso, dass die Ideale $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{r}$ notwendig unter einander verschieden sind; damit ist auch der letzte Teil des Satzes 105 bewiesen.

§ 74.

Die ambigen Idealklassen.

Wenn $\mathfrak{a}$ ein Ideal der Klasse A ist, so werde diejenige Idealklasse, der das Ideal $s\mathfrak{a}$ angehört, mit sA bezeichnet. Ist insbesondere $A = sA$, so heisst die Idealklasse A eine **ambige Idealklasse.** Da das Product $\mathfrak{a}.s\mathfrak{a} \sim 1$ ist, so wird $A.sA = 1$; und folglich ist das Quadrat einer jeden ambigen Klasse gleich der Hauptklasse 1. Umgekehrt, wenn das Quadrat einer Klasse A gleich 1 ist, so wird $A = \frac{1}{A} = sA$, und folglich ist A eine ambige Klasse.

§ 75.

Die durch ambige Ideale bestimmten ambigen Idealklassen.

Es entsteht nun die Aufgabe, alle ambigen Klassen in k aufzustellen. Da offenbar ein jedes ambige Ideal $\mathfrak{a}$ vermöge seiner Eigenschaft $\mathfrak{a} = s\mathfrak{a}$ eine ambige Klasse bestimmt, so haben wir vor allem zu untersuchen, wie viele von einander verschiedene ambige Klassen aus den 2^t ambigen Idealen entspringen. Wir bezeichnen allgemein irgend welche vorgelegte Idealklassen als **von einander unabhängige Idealklassen,** wenn keine darunter die Klasse 1 ist und auch keine gleich einem Producte von Potenzen der übrigen dieser Klassen gesetzt werden kann. Wir sprechen dann folgende Thatsache aus:

Satz 106. Die t ambigen Primideale bestimmen im Falle eines imaginären Körpers stets $t-1$ von einander unabhängige ambige Klassen; im Falle eines reellen Körpers bestimmen sie $t-2$ oder $t-1$ von ein-

ander unabhängige ambige Klassen, je nachdem die Norm der Grundeinheit ε des Körpers $n(\varepsilon) = +1$ oder $= -1$ ist. Die sämtlichen 2^t ambigen Ideale bestimmen im Falle eines imaginären Körpers 2^{t-1} und im Falle eines reellen Körpers, entsprechend der eben gemachten Unterscheidung, 2^{t-2} bez. 2^{t-1} von einander verschiedene ambige Klassen.

Beweis. Das Product aus sämtlichen in m aufgehenden Primidealen ist gleich $\sqrt{m}$ und mithin ein Hauptideal in k. Ist zunächst m negativ, jedoch von -1 und -3 verschieden, und (α) ein ambiges Hauptideal in k, so muss α^{1-s} als Einheit notwendig $= (-1)^e$ sein, wo e die Werte 0 oder 1 haben kann; hieraus folgt:

$$\{\alpha(\sqrt{m})^e\}^{1-s} = 1 \quad \text{oder} \quad \alpha(\sqrt{m})^e = s\{\alpha(\sqrt{m})^e\},$$

d. h. $\alpha(\sqrt{m})^e$ ist dann eine ganze rationale Zahl. Damit ist bewiesen, dass in einem imaginären Körper $k(\sqrt{m})$ — von $k(\sqrt{-1})$ und $k(\sqrt{-3})$ abgesehen — gewiss ausser 1 und $\sqrt{m}$ kein ambiges Hauptideal vorhanden ist. Die beiden hier zunächst ausgeschlossenen Fälle erledigen sich unmittelbar im Sinne des zu beweisenden Satzes 106.

Bei der Entscheidung der fraglichen Verhältnisse für einen reellen Körper k kommt es darauf an, ob die Norm der Grundeinheit ε des Körpers gleich $+1$ oder -1 ausfällt.

Ist nämlich $n(\varepsilon) = +1$, so kann man nach Satz 90 die Formel $\varepsilon = \alpha^{1-s}$ durch eine ganze Zahl α in k befriedigen und noch α ohne rationalen Factor $\neq \pm 1$ voraussetzen. Wegen $\alpha = \varepsilon \cdot s\alpha$ ist dann (α) ein ambiges Hauptideal. Dieses Hauptideal (α) ist von 1 und von $\sqrt{m}$ verschieden; denn wäre $\alpha = \pm\varepsilon^f$ oder $= \pm\varepsilon^f\sqrt{m}$, wo der Exponent f eine ganze rationale Zahl bedeutet, so würde

$$\alpha^{1-s} = (-1)^e \varepsilon^{(1-s)f} = (-1)^e \varepsilon^{2f} \quad (e = 0 \text{ bez. } 1)$$

folgen; letzterer Ausdruck aber ist stets von ε verschieden. Ist ferner α' ein beliebiges ambiges Hauptideal des Körpers k, so ist notwendigerweise $\alpha'^{1-s} = (-1)^e \varepsilon^f$, wo die Exponenten e und f ganze rationale Zahlen bedeuten. Setzen wir $\alpha'' = \dfrac{\alpha'}{(\sqrt{m})^e \alpha^f}$, so folgt $\alpha''^{1-s} = 1$, d. h. α'' ist eine rationale Zahl, und danach giebt es ausser 1, $\sqrt{m}$ und α nur noch ein ambiges Hauptideal, das durch Befreiung des Products $\sqrt{m} \cdot \alpha$ von etwaigen ganzen rationalen Factoren $\neq \pm 1$ entsteht.

Ist andererseits $n(\varepsilon) = -1$, so giebt es kein von 1 und $\sqrt{m}$ verschiedenes ambiges Hauptideal in k; denn ist (α) ein beliebiges ambiges Hauptideal in k, so gilt notwendigerweise eine Gleichung $\alpha^{1-s} = (-1)^e \varepsilon^f$

mit ganzen rationalen e, f; wegen $n(\alpha^{1-s}) = +1$ ergiebt sich $(n(\varepsilon))^f = +1$, d. h. f ist eine gerade Zahl. Setzen wir $\alpha' = \frac{\alpha}{\varepsilon^{\frac{f}{2}} (\sqrt{m})^{e+\frac{f}{2}}}$, so folgt $\alpha'^{1-s} = +1$, d. h. α' ist eine rationale Zahl.

Wir drücken nun von den t ambigen Primidealen in k ein geeignetes durch $\sqrt{m}$ und die $t-1$ übrigen ambigen Primideale und, wenn der Körper k reell und zugleich $n(\varepsilon) = +1$ ausfällt, weiter noch von diesen $t-1$ ambigen Primidealen ein geeignetes durch α und die $t-2$ übrigen dieser Ideale aus. Hierdurch erkennen wir die Richtigkeit des zweiten Teiles des Satzes 106.

§ 76.

Die ambigen Idealklassen, welche kein ambiges Ideal enthalten.

Es gilt die folgende Thatsache:

Satz 107. Es giebt im quadratischen Körper k dann und nur dann eine ambige Klasse, welche kein ambiges Ideal enthält, wenn der Körper k reell ist, das Charakterensystem von -1 in ihm aus lauter positiven Einheiten besteht und endlich die Norm der Grundeinheit gleich $+1$ ausfällt. Sind diese Bedingungen erfüllt, so entstehen alle überhaupt vorhandenen Klassen von jener Beschaffenheit dadurch, dass man eine beliebige unter ihnen der Reihe nach mit allen aus den ambigen Idealen entspringenden Klassen multiplicirt.

Beweis. Wenn der Körper k reell ist und das Charakterensystem von -1 in ihm aus lauter positiven Einheiten besteht, so giebt es nach Satz 102 in k stets eine ganze oder gebrochene Zahl α, deren Norm $= -1$ wird. Ist ferner die Norm der Grundeinheit $n(\varepsilon) = +1$, so ist diese Zahl α notwendig eine gebrochene. Setzen wir $\alpha = \frac{\mathfrak{j}}{\mathfrak{j}'}$, wo $\mathfrak{j}$ und $\mathfrak{j}'$ zu einander prime Ideale sein sollen, so wird $\frac{\mathfrak{j} \cdot s\mathfrak{j}}{\mathfrak{j}' \cdot s\mathfrak{j}'} = 1$, und hieraus folgt $\mathfrak{j}' = s\mathfrak{j}$, also $\mathfrak{j} \sim s\mathfrak{j}$, und $\mathfrak{j}$ bestimmt folglich eine ambige Klasse. Diese ambige Klasse enthält kein ambiges Ideal. Wäre nämlich ein Ideal $\mathfrak{a} = \mathfrak{j}\beta$, wo β eine ganze oder gebrochene Zahl des Körpers k bedeutet, ambig, so würde $\mathfrak{a}^{1-s} = \alpha\beta^{1-s}$ folgen, und mithin wäre $\alpha\beta^{1-s}$ gleich einer Einheit, etwa $= (-1)^e \varepsilon^f$, und folglich $n(\alpha) = +1$, was der Construction der Zahl α zuwiderliefe. Damit ist bewiesen, dass die durch $\mathfrak{j}$ bestimmte ambige Klasse kein ambiges Ideal enthält.

Es sei jetzt A eine beliebig gegebene ambige Klasse und $\mathfrak{j}$ ein Ideal derselben, so ist $\mathfrak{j}^{1-s}$ gleich einer ganzen oder gebrochenen Zahl α des Körpers k, und es wird die Norm $n(\alpha)$ entweder $=+1$ oder $=-1$ sein. Der erstere Fall ist der einzig mögliche, wenn der Körper k imaginär ist, oder wenn der Körper k reell ist und wenigstens einer von den Charakteren $\left(\frac{-1, m}{w}\right)$ den Wert -1 besitzt. Sowie nun $n(\alpha)=+1$ ist, folgt nach Satz 90, dass $\frac{1}{\alpha}=\beta^{1-s}$ wird, wo β eine ganze Zahl β in k bedeutet; dann ist $(\mathfrak{j}\beta)^{1-s}=1$, d. h. $\mathfrak{j}\beta$ gleich dem Product eines ambigen Ideals in eine rationale Zahl, und die Klasse A enthält mithin ein ambiges Ideal. Ist andererseits $n(\alpha)=-1$ und zugleich $n(\varepsilon)=-1$, so wird $n(\varepsilon\alpha)=+1$, und wir beweisen wie vorhin, dass die Klasse A ein ambiges Ideal enthält. Daraus ersehen wir, dass jede ambige Klasse ein ambiges Ideal enthält, falls der Körper k imaginär ist, und desgleichen, falls der Körper k reell ist und für ihn entweder einer der Charaktere von -1 den Wert -1 besitzt oder $n(\varepsilon)=-1$ ausfällt.

Nehmen wir endlich in dem weiteren Falle, dass keiner dieser Umstände zutrifft, an, es gebe in k mehrere ambige Idealklassen, die kein ambiges Ideal enthalten, und wählen aus zweien darunter je ein Ideal, $\mathfrak{j}$ und $\mathfrak{j}'$, aus, so zeigt die vorhin dargelegte Entwickelung, dass die Normen der beiden Zahlen $\alpha=\mathfrak{j}^{1-s}$ und $\alpha'=\mathfrak{j}'^{1-s}$ notwendig den Wert -1 besitzen, und es wird folglich $n\left(\frac{\alpha'}{\alpha}\right)=+1$. Nach Satz 90 ergiebt sich hieraus eine Darstellung $\frac{\alpha}{\alpha'}=\beta^{1-s}$ mit Hülfe einer geeigneten ganzen Zahl β in k. Setzen wir $\frac{\mathfrak{j}'\beta}{\mathfrak{j}}=b\mathfrak{a}$, wo b eine rationale Zahl und $\mathfrak{a}$ ein Ideal ohne ganzen rationalen Factor $\neq\pm 1$ bedeute, so folgt wegen $\left(\frac{\mathfrak{j}'\beta}{\mathfrak{j}}\right)^{1-s}=1$ die Gleichung $\mathfrak{a}=s\mathfrak{a}$, d. h. $\mathfrak{a}$ ist ein ambiges Ideal; und dabei ist $\mathfrak{j}' \sim \mathfrak{a}\mathfrak{j}$. Damit haben wir auch den letzten Teil unseres Satzes 107 bewiesen.

§ 77.

Die Anzahl aller ambigen Klassen.

Die Sätze 106 und 107 ermöglichen die Berechnung der Anzahl aller ambigen Klassen.

Satz 108. Es giebt in jedem Falle im Körper k genau $r-1$ von

einander unabhängige ambige Klassen, wo r die Anzahl der Einzelcharaktere bedeutet, die das Geschlecht einer Klasse bestimmen. Die Anzahl der sämtlichen von einander verschiedenen ambigen Klassen ist daher gleich 2^{r-1}.

Beweis. Es sei wieder t die Anzahl der verschiedenen in der Discriminante d des Körpers k aufgehenden rationalen Primzahlen. Betrachten wir zunächst den Fall, dass k ein imaginärer Körper ist, so folgt aus den Sätzen 106 und 107 das Vorhandensein von genau 2^{t-1} ambigen Klassen in k; diese entspringen sämtlich aus ambigen Idealen. Jetzt sei der Körper k reell; besteht das Charakterensystem der Zahl -1 in k aus lauter positiven Einheiten, so folgt desgleichen aus den Sätzen 106 und 107 das Vorhandensein von genau 2^{t-1} ambigen Klassen in k; von diesen 2^{t-1} ambigen Klassen entspringen hier entweder sämtliche oder nur die Hälfte aus ambigen Idealen, je nachdem $n(\varepsilon) = -1$ oder $= +1$ ausfällt. Besitzt jedoch die Zahl -1 für k wenigstens einen negativen Charakter, so ist stets $n(\varepsilon) = +1$; nach den Sätzen 106 und 107 giebt es dann nur 2^{t-2} ambige Klassen in k, und diese entspringen sämtlich aus ambigen Idealen. Nun ist die Anzahl r der Einzelcharaktere $= t-1$, wenn der Körper k reell ist und überdies die Zahl -1 für k wenigstens einen negativen Charakter besitzt; es ist $r = t$ in jedem anderen Falle; damit ist unser Satz 108 bewiesen.

§ 78.

Der arithmetische Beweis für die Existenz der Geschlechter.

Die gewonnenen Resultate setzen uns in den Stand, auf die Frage nach der Anzahl der Geschlechter die Antwort zu finden, die im Fundamentalsatze 100 ausgesprochen ist; wir können nämlich beweisen, dass diese Anzahl stets gleich 2^{r-1} ist, und dass mithin alle diejenigen Charakterensysteme, die der Bedingung des Satzes 100 Genüge leisten, wirklich unter den Geschlechtern vertreten sind. Wir bezeichnen die Anzahl der von einander verschiedenen existirenden Geschlechter mit g und die Anzahl der Klassen des Hauptgeschlechtes mit f. Da nach § 66 alle Geschlechter die gleiche Anzahl von Klassen enthalten, so ist die Anzahl h sämtlicher Klassen des Körpers $h = gf$. Bezeichnen wir ferner die f Klassen des Hauptgeschlechtes mit $H_1, \ldots, H_f$, so können wir nach dem Satze 103 $H_1 = K_1^2, \ldots, H_f = K_f^2$ setzen, wo $K_1, \ldots, K_f$ gewisse f Klassen des Körpers bedeuten.

Es sei jetzt C eine beliebige Klasse des Körpers; da C^2 offenbar zum Hauptgeschlecht gehört, so ist $C^2 = K_a^2$, wo K_a eine ganz bestimmte der eben eingeführten Klassen $K_1, \ldots, K_f$ bedeutet. Es ist dann $\frac{C}{K_a}$, d. h. diejenige wieder ganz bestimmte Klasse A, für welche $C = AK_a$ wird, eine ambige Klasse, und es stellt also der Ausdruck AK, wenn A alle ambigen Klassen und K die Klassen $K_1, \ldots, K_f$ durchläuft, eine jede überhaupt vorhandene Idealklasse des Körpers dar, und auch jede nur auf eine Weise. Da nach Satz 108 die Anzahl der ambigen Klassen 2^{r-1} beträgt, so ergiebt sich $h = 2^{r-1}f$, und es führt die Zusammenstellung dieser Gleichung mit der oben gefundenen $h = gf$ zu der Beziehung $g = 2^{r-1}$. Damit ist der Fundamentalsatz 100 vollständig bewiesen. [*Gauss*[1].]

§ 79.

Die transcendente Darstellung der Klassenanzahl und eine Anwendung darauf, dass der Grenzwert eines gewissen unendlichen Productes positiv ist.

Der zweite Beweis für die Existenz der 2^{r-1} Geschlechter beruht auf transcendenter Grundlage; wir entwickeln der Reihe nach die folgenden Sätze:

Satz 109. Die Anzahl h der Idealklassen des quadratischen Körpers k mit der Discriminante d bestimmt sich durch folgende Formel:

$$\varkappa h = \underset{s=1}{L} \underset{(p)}{\Pi} \frac{1}{1 - \left(\frac{d}{p}\right) p^{-s}}.$$

Hierin ist das Product rechter Hand über alle rationalen Primzahlen p zu erstrecken, und das Symbol $\left(\frac{d}{p}\right)$ hat die in § 61 festgesetzte Bedeutung. Für den Factor $\varkappa$ gilt, je nachdem der Körper k imaginär oder reell, also d negativ oder positiv ist:

$$\varkappa = \frac{2\pi}{w|\sqrt{d}|} \quad \text{bez.} \quad \varkappa = \frac{2 \log \varepsilon}{|\sqrt{d}|}.$$

Dabei bedeutet w für $d = -3$ die Zahl 6, für $d = -4$ die Zahl 4, für jedes andere negative d die Zahl 2; andererseits verstehe man für einen reellen Körper k unter ε jetzt speciell diejenige seiner vier Grund-

einheiten, welche >1 ist, und unter $\log \varepsilon$ den reellen Wert des Logarithmus dieser Grundeinheit ε. [*Dirichlet*[8, 9].]

Beweis. Nach § 27 gilt, solange s reell und >1 ist:

$$\zeta(s) = \sum_{(\mathfrak{j})} \frac{1}{n(\mathfrak{j})^s} = \prod_{(\mathfrak{p})} \frac{1}{1-n(\mathfrak{p})^{-s}},$$

wo das Product über alle Primideale $\mathfrak{p}$ des Körpers k zu erstrecken ist. Ordnen wir dieses Product nach den rationalen Primzahlen p, aus welchen die Primideale $\mathfrak{p}$ herstammen, so gehört, wie aus Satz 97 folgt, zu einer beliebigen rationalen Primzahl p in dem Producte das Glied:

$$\frac{1}{(1-p^{-s})^2} \quad \text{oder} \quad \frac{1}{1-p^{-2s}} \quad \text{oder} \quad \frac{1}{1-p^{-s}},$$

je nachdem $\left(\frac{d}{p}\right) = +1, = -1, = 0$ ist. Wir schreiben diese drei Ausdrücke in der ihnen gemeinschaftlichen Form:

$$\frac{1}{1-p^{-s}} \frac{1}{1-\left(\frac{d}{p}\right)p^{-s}}$$

und erhalten so:

$$\zeta(s) = \prod_{(p)} \frac{1}{1-p^{-s}} \prod_{(p)} \frac{1}{1-\left(\frac{d}{p}\right)p^{-s}},$$

wo die beiden Producte rechter Hand über alle rationalen Primzahlen p zu erstrecken sind. Wegen

$$\underset{s=1}{L}\left\{(s-1)\prod_{(p)} \frac{1}{1-p^{-s}}\right\} = \underset{s=1}{L}\left\{(s-1)\sum_{(n)} \frac{1}{n^s}\right\} = 1,$$

wo n alle positiven ganzen rationalen Zahlen durchläuft, wird dann:

$$\underset{s=1}{L}\{(s-1)\zeta(s)\} = \underset{s=1}{L} \prod_{(p)} \frac{1}{1-\left(\frac{d}{p}\right)p^{-s}}.$$

Die Richtigkeit unseres Satzes 109 folgt nun aus Satz 56, wenn wir den Wert von $\varkappa$ nach § 25 aufstellen. Zur Ermittelung von w ist zu berücksichtigen, dass der Körper $k(\sqrt{-3})$ die 6 Einheitswurzeln ± 1, $\pm \frac{1 \pm \sqrt{-3}}{2}$, der Körper $k(\sqrt{-1})$ die 4 Einheitswurzeln $\pm 1, \pm i$, dagegen ein jeder

andere imaginäre quadratische Körper k nur die beiden Einheitswurzeln ± 1 enthält. (Vgl. § 62.)

Die wichtigste Folgerung der eben bewiesenen Thatsache ist der Satz:

Satz 110. Bedeutet a eine beliebige ganze rationale positive oder negative Zahl, nur nicht eine Quadratzahl, so ist der Grenzwert

$$\underset{s=1}{L} \prod_{(p)} \frac{1}{1-\left(\frac{a}{p}\right)p^{-s}}$$

stets eine endliche und von 0 verschiedene Grösse. [*Dirichlet*[8, 9].]

Beweis. Es sei $a = b^2 m$, wo b^2 die grösste in a aufgehende Quadratzahl sein soll; es sei ferner d die Discriminante des durch $\sqrt{a}$ bestimmten quadratischen Körpers. Dann folgt für jede ungerade und nicht in b aufgehende rationale Primzahl p gewiss die Gleichung $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right)$. Die beiden unendlichen Producte

$$\prod_{(p)} \frac{1}{1-\left(\frac{d}{p}\right)p^{-s}} \quad \text{und} \quad \prod_{(p)} \frac{1}{1-\left(\frac{a}{p}\right)p^{-s}}$$

können demnach nur in einer endlichen Anzahl von Factoren von einander abweichen. Da das erstere Product nach Satz 109 in der Grenze für $s = 1$ endlich bleibt, so gilt daher dasselbe auch von dem zweiten Product.

§ 80.

Das Vorhandensein unendlich vieler rationaler Primzahlen, nach denen gegebene Zahlen vorgeschriebene quadratische Restcharaktere erlangen.

Mit Hülfe des Satzes 110 beweisen wir der Reihe nach folgende Thatsachen: [*Dirichlet*[9], *Kronecker*[10].]

Satz 111. Bedeuten $a_1, a_2, \ldots, a_t$ irgend t ganze rationale, positive oder negative Zahlen von der Art, dass keine der 2^t-1 Zahlen $a_1, a_2, \ldots, a_t, a_1a_2, \ldots, a_{t-1}a_t, \ldots, a_1a_2\ldots a_t$ eine Quadratzahl wird, und sind $c_1, c_2, \ldots, c_t$ nach Belieben vorgeschriebene Einheiten $+1$ oder -1, so giebt es stets unendlich viele rationale Primzahlen p, für die

$$\left(\frac{a_1}{p}\right) = c_1, \quad \left(\frac{a_2}{p}\right) = c_2, \quad \ldots, \quad \left(\frac{a_t}{p}\right) = c_t$$

ist.

Beweis. Wir haben, solange $s > 1$ ist:

$$\log \sum_{(n)} \frac{1}{n^s} = \sum_{(p)} \log \frac{1}{1-p^{-s}} = \sum_{(p)} \frac{1}{p^s} + S,$$

$$S = \tfrac{1}{2} \sum_{(p)} \frac{1}{p^{2s}} + \tfrac{1}{3} \sum_{(p)} \frac{1}{p^{3s}} + \cdots$$

Da der Ausdruck S, wie in § 50 gezeigt worden ist, für $s = 1$ endlich bleibt, so folgt, dass die über alle rationalen Primzahlen p erstreckte Summe

$$(26.) \qquad \sum_{(p)} \frac{1}{p^s}$$

bei Annäherung von s an 1 über alle Grenzen wächst. Ist ferner a eine beliebige ganze rationale Zahl, so gilt ähnlich für $s > 1$ stets:

$$\log \prod_{(p)} \frac{1}{1 - \left(\frac{a}{p}\right) p^{-s}} = \sum_{(p)} \left(\frac{a}{p}\right) \frac{1}{p^s} + S_a,$$

$$S_a = \tfrac{1}{2} \sum_{(p)} \left(\frac{a}{p}\right)^2 \frac{1}{p^{2s}} + \tfrac{1}{3} \sum_{(p)} \left(\frac{a}{p}\right)^3 \frac{1}{p^{3s}} + \cdots;$$

ist a nicht eine Quadratzahl, so bleibt nach Satz 110 $\log \prod_{(p)} \frac{1}{1 - \left(\frac{a}{p}\right) p^{-s}}$ für $s = 1$ endlich, und da das Gleiche von dem Ausdruck S_a gilt, so folgt, dass dann auch die Summe

$$(27.) \qquad \sum_{(p)} \left(\frac{a}{p}\right) \frac{1}{p^s}$$

für $s = 1$ sich einer endlichen Grenze nähert. Wir setzen nun in (27.)

$$a = a_1^{u_1} a_2^{u_2} \ldots a_t^{u_t}$$

ein und geben jedem der t Exponenten $u_1, u_2, \ldots, u_t$ den Wert 0 oder 1, jedoch so, dass das Wertsystem $u_1 = 0, u_2 = 0, \ldots, u_t = 0$ ausgeschlossen bleibt. Wird dann jede so aus (27.) herzuleitende Summe noch mit dem entsprechenden Factor $c_1^{u_1} c_2^{u_2} \ldots c_t^{u_t}$ multiplicirt, und werden die hervorgehenden $2^t - 1$ Ausdrücke sämtlich zu (26.) addirt, so entsteht:

$$(28.) \qquad \sum_{(p)} \left(1 + c_1 \left(\frac{a_1}{p}\right)\right) \left(1 + c_2 \left(\frac{a_2}{p}\right)\right) \cdots \left(1 + c_t \left(\frac{a_t}{p}\right)\right) \frac{1}{p^s}.$$

Diese Summe wird, ebenso wie (26.), bei Annäherung von s an 1 über

alle Grenzen wachsen. Sehen wir von den Gliedern ab, die den in $a_1 a_2 \ldots a_t$ aufgehenden Primzahlen p entsprechen, und die nur in endlicher Anzahl vorhanden sind, so ist im übrigen die Summe (28.) gleich $2^t \sum\limits_{(p')} \frac{1}{p'^s}$, wo p' nur alle diejenigen Primzahlen p durchläuft, für welche die im Satze 111 verlangten Bedingungen sämtlich erfüllt sind. Da mithin auch diese letzte Summe für $s = 1$ über alle Grenzen wächst, so folgt, dass jene Primzahlen p' in unendlicher Anzahl vorhanden sein müssen. Damit ist Satz 111 bewiesen.

§ 81.

Das Vorhandensein unendlich vieler Primideale mit vorgeschriebenen Charakteren in einem quadratischen Körper.

Satz 112. Sind

$$\chi_1(\mathfrak{j}) = \left(\frac{\pm n(\mathfrak{j}), m}{l_1}\right), \quad \ldots, \quad \chi_r(\mathfrak{j}) = \left(\frac{\pm n(\mathfrak{j}), m}{l_r}\right)$$

die r Einzelcharaktere, welche das Geschlecht eines Ideals $\mathfrak{j}$ in k bestimmen, und bedeuten $c_1, \ldots, c_r$ beliebig angenommene, der Bedingung $c_1 \ldots c_r = +1$ genügende r Einheiten ± 1, so giebt es stets unendlich viele Primideale $\mathfrak{p}$ im Körper k, für welche

$$\chi_1(\mathfrak{p}) = c_1, \quad \ldots, \quad \chi_r(\mathfrak{p}) = c_r$$

ist.

Beweis. In der Discriminante d des Körpers seien die t rationalen Primzahlen $l_1, \ldots, l_t$ enthalten. Es ist $t = r$ oder $= r+1$; in letzterem Falle sei $\left(\frac{-1, m}{l_t}\right) = -1$, und die Bedingung $\left(\frac{\pm n(\mathfrak{j}), m}{l_t}\right) = +1$ diene zur Bestimmung des Vorzeichens in $\pm n(\mathfrak{j})$. Zugleich schreiben wir in diesem Falle $c_t = c_{r+1} = +1$. Wir beweisen nun zunächst, dass es unendlich viele rationale Primzahlen p giebt, für welche

$$\left(\frac{p, m}{l_1}\right) = c_1, \quad \ldots, \quad \left(\frac{p, m}{l_t}\right) = c_t$$

ist, und unterscheiden zu dem Zweck drei Fälle, je nachdem $m \equiv 1$, $\equiv 3$, oder $\equiv 2$ nach 4 ist.

Im ersten Falle gehen wir von den Forderungen

$$\left(\frac{-1}{p}\right) = +1, \quad \left(\frac{l_1}{p}\right) = c_1, \quad \ldots, \quad \left(\frac{l_t}{p}\right) = c_t$$

aus. Nach Satz 111 giebt es unendlich viele Primzahlen p, welche diesen Gleichungen genügen. Da die erste Gleichung auf $p \equiv 1$ nach 4 hinauskommt, so wird für diese Primzahlen p dann

$$\left(\frac{p,m}{l_i}\right)=\left(\frac{p}{l_i}\right)=\left(\frac{l_i}{p}\right)=c_i$$

für $i=1,\ldots,t$ gelten.

Im zweiten Falle sei unter den Primzahlen $l_1,\ldots,l_t$ etwa l_z die Primzahl 2. Ist dann $c_z=+1$, so legen wir die Forderungen

$$\left(\frac{-1}{p}\right)=+1,\quad \left(\frac{l_i}{p}\right)=c_i \qquad (i=1,\ldots,z-1,z+1,\ldots,t)$$

zu Grunde, und es folgt nach Satz 111, dass es unendlich viele diesen Gleichungen genügende Primzahlen p giebt. Wegen der ersten Gleichung wird $\left(\frac{p,m}{2}\right)=+1=c_z$ und überdies $\left(\frac{p,m}{l_i}\right)=\left(\frac{p}{l_i}\right)=\left(\frac{l_i}{p}\right)=c_i$ für $i=1,\ldots,z-1,z+1,\ldots,t$. Ist dagegen $c_z=-1$, so fordern wir:

$$\left(\frac{-1}{p}\right)=-1,\quad \left(\frac{l_i}{p}\right)=(-1)^{\frac{l_i-1}{2}}c_i,\qquad (i=1,\ldots,z-1,z+1,\ldots,t)$$

und die unendlich vielen, diesen Gleichungen genügenden Primzahlen p erfüllen zugleich die Bedingungen:

$$\left(\frac{p,m}{2}\right)=-1=c_z \quad\text{und}\quad \left(\frac{p,m}{l_i}\right)=\left(\frac{p}{l_i}\right)=(-1)^{\frac{l_i-1}{2}}\left(\frac{l_i}{p}\right)=c_i$$

für $i=1,\ldots,z-1,z+1,\ldots,t$.

Im dritten Falle endlich suchen wir wieder $l_z=2$ heraus. Wir stellen die Forderungen:

$$\left(\frac{-1}{p}\right)=+1,\quad \left(\frac{2}{p}\right)=c_z,\quad \left(\frac{l_i}{p}\right)=c_i,\quad (i=1,\ldots,z-1,z+1,\ldots,t);$$

es existiren nach Satz 111 unendlich viele Primzahlen p, welche ihnen genügen, und für welche dann

$$\left(\frac{p,m}{2}\right)=(-1)^{\frac{p^2-1}{8}+\frac{p-1}{2}\frac{\frac{m}{2}-1}{2}}=(-1)^{\frac{p^2-1}{8}}=\left(\frac{2}{p}\right)=c_z$$

und überdies $\left(\frac{p,m}{l_i}\right)=\left(\frac{p}{l_i}\right)=\left(\frac{l_i}{p}\right)=c_i$ für $i=1,\ldots,z-1,$ $z+1,\ldots,t$ wird.

Es bedeute nun p eine beliebige solche rationale Primzahl, dass

$$\left(\frac{p, m}{l_1}\right) = c_1, \quad \ldots, \quad \left(\frac{p, m}{l_t}\right) = c_t$$

gilt. Nach Hülfssatz 14 ist dann

$$\underset{(w)}{\Pi}\left(\frac{p, m}{w}\right) = \left(\frac{p, m}{p}\right)\left(\frac{p, m}{l_1}\right)\cdots\left(\frac{p, m}{l_t}\right) = +1,$$

und folglich

$$\left(\frac{m}{p}\right) c_1 \ldots c_t = \left(\frac{m}{p}\right) = +1;$$

also findet man p im Körper k in das Product zweier Primideale $\mathfrak{p}$ und $\mathfrak{p}'$ zerlegbar. Jedes dieser Primideale $\mathfrak{p}$ und $\mathfrak{p}'$ erfüllt die Bedingungen des zu beweisenden Satzes 112.

§ 82.

Der transcendente Beweis für die Existenz der Geschlechter und für die übrigen in § 71 bis § 77 erlangten Resultate.

Der Satz 112 zeigt nicht nur die Existenz der 2^{r-1} Geschlechter von neuem, sondern er deckt zugleich eine andere tiefer liegende Thatsache auf:

Satz 113. Unter den Idealen eines beliebigen Geschlechtes im quadratischen Körper giebt es stets unendlich viele Primideale.

Hat man den Satz von der Existenz der 2^{r-1} Geschlechter auf dem zweiten transcendenten Wege unabhängig von den Sätzen 102, 103 und 108 festgestellt, so ist es leicht, nachträglich auch diese Sätze zu gewinnen. Man hat nämlich dazu nur noch die Kenntnis der Thatsache nötig, dass die Anzahl a der ambigen Klassen in k jedenfalls $\leqq 2^{r-1}$ ist. Diese Thatsache folgt aus Satz 106 über die Anzahl derjenigen ambigen Klassen, welche aus ambigen Idealen entspringen, in Verbindung mit den Schlüssen im zweiten und dritten Absatz des Beweises zu Satz 107; sie steht bei solcher Ableitung völlig unabhängig von Satz 102 da.

Es bezeichne dann, wie oben, f die Anzahl der Klassen des Hauptgeschlechtes, g die Anzahl der Geschlechter und ferner f' die Anzahl derjenigen unter den f Klassen des Hauptgeschlechtes, welche gleich Quadraten von Klassen sind. Es folgt wie in § 78, dass $gf = af'$ ist, und da nunmehr bereits $g = 2^{r-1}$ bewiesen, ferner $a \leqq 2^{r-1}$ sicher ist, und selbstverständlich $f' \leqq f$ besteht, so ergiebt sich hieraus $f' = f$ und

$a = 2^{r-1}$. Die erste Gleichung beweist den Satz 103, die zweite den Satz 108 und sodann den Satz 102 für $n = -1$. Aus Satz 103 und dem letzten Ergebnisse endlich folgt der Satz 102 vollständig. Denn die Zahl n darin ist wegen der für sie gestellten Bedingungen gleich der Norm eines Ideals $\mathfrak{h}$ des Hauptgeschlechtes, versehen mit einem Vorzeichen in der in § 65 festgesetzten Weise. Bedeutet dann $\mathfrak{k}$ ein solches Ideal, dass $\mathfrak{h} \sim \mathfrak{k}^2$ ist, so muss $\alpha = \frac{\mathfrak{h} . n(\mathfrak{k})}{\mathfrak{k}^2}$ eine ganze oder gebrochene Zahl des Körpers k sein, und zwar ergiebt sich $n(\alpha) = \pm n$, woraus der Satz 102 folgt, sobald man berücksichtigt, dass er für $n = -1$ gilt.

So sind durch die zuletzt entwickelte transcendente Methode die Resultate in § 71 — § 78 gerade in umgekehrter Reihenfolge zum Nachweise gelangt, als sie auf dem zuerst eingeschlagenen rein arithmetischen Wege gefunden wurden.

§ 83.

Die engere Fassung des Aequivalenz- und Klassenbegriffes.

Wenn wir den in § 24 dargelegten engeren Begriff der Aequivalenz zweier Ideale zu Grunde legen, so erfahren die in den Capiteln XVII und XVIII aufgestellten Sätze nur einfache, leicht zu ermittelnde Modificationen.

Zunächst ist klar, dass der engere Aequivalenzbegriff in einem imaginären Körper k unter allen Umständen und in einem reellen Körper k sicherlich immer dann mit dem ursprünglichen Aequivalenzbegriffe zusammenfällt, wenn für den Körper die Norm der Grundeinheit $n(\varepsilon) = -1$ ist. Wenn aber k reell ist und $n(\varepsilon) = +1$ aufweist, so löst sich eine Idealklasse im Sinne der früheren Einteilung bei der neuen Einteilung regelmässig in zwei Klassen auf; insbesondere entstehen aus der früheren Klasse der Hauptideale die zwei durch das Hauptideal (1) und durch das Hauptideal $(\sqrt{m})$ vertretenen Klassen der neuen Einteilung. Bezeichnet h' die Anzahl der Idealklassen bei Benutzung des engeren Aequivalenzbegriffes, so ist daher unter den gegenwärtig angenommenen Umständen $h' = 2h$. [*Dedekind* [1].]

§ 84.

Der Fundamentalsatz für den neuen Klassen- und Geschlechtsbegriff.

Dem neuen Klassenbegriff entspricht ein neuer Geschlechtsbegriff: das Geschlecht eines Ideals $\mathfrak{j}$ im Körper $k(\sqrt{m})$ soll nämlich nunmehr in

allen Fällen gleichmässig durch die t Einheiten

$$\left(\frac{+n(\mathfrak{j}), m}{l_1}\right), \quad \ldots, \quad \left(\frac{+n(\mathfrak{j}), m}{l_t}\right)$$

charakterisirt werden, wo die Norm von $\mathfrak{j}$ im Unterschiede von der früheren Festsetzung stets das positive Vorzeichen erhält. Für einen imaginären Körper k stimmt dieser neue Geschlechtsbegriff mit dem alten völlig überein. Das Gleiche gilt für einen reellen Körper k, falls das Charakterensystem der Zahl -1 in k aus lauter positiven Einheiten besteht. Der letztere Umstand muss offenbar immer eintreten, wenn für k die Norm der Grundeinheit $= -1$ ist. Nun sei k reell und für k die Norm der Grundeinheit $= +1$, so sind zwei Fälle zu unterscheiden, je nachdem das Charakterensystem der Zahl -1 in k aus lauter positiven Einheiten besteht oder nicht.

Im ersteren Falle gehören die Ideale (1) und $\mathfrak{a} = (\sqrt{m})$ beide zum nämlichen Geschlechte, da sich

$$\left(\frac{n(\mathfrak{a}), m}{l_i}\right) = \left(\frac{+m, m}{l_i}\right) = \left(\frac{+m, m}{l_i}\right)\left(\frac{-1, m}{l_i}\right) = \left(\frac{-m, m}{l_i}\right) = +1$$

für $i = 1, \ldots, t$ ergiebt. Die neuen Geschlechter umfassen also die nämlichen Ideale wie die alten, und die Zahl der Geschlechter ist wiederum $= 2^{t-1}$.

Im zweiten Falle gehören die beiden Idealklassen, welche durch das Ideal (1) und durch das Ideal $\mathfrak{a} = (\sqrt{m})$ repräsentirt werden, zu verschiedenen der neuen Geschlechter. Die Anzahl der neuen Geschlechter ist doppelt so gross, als die der alten; nun war für diesen Fall die Anzahl der Einzelcharaktere bei Zugrundelegung des ursprünglichen Geschlechtsbegriffs nur $= t-1$ und die Anzahl der alten Geschlechter daher $= 2^{t-2}$; es ergiebt sich somit die Anzahl der neuen Geschlechter, ebenso wie im ersten Falle, $= 2^{t-1}$. Da ferner in jedem Falle das Product

$$\left(\frac{-1, m}{l_1}\right) \cdots \left(\frac{-1, m}{l_t}\right) = +1$$

ist, so gilt der Fundamentalsatz 100 auch bei Zugrundelegung des neuen Klassenbegriffes mit dem entsprechenden Geschlechtsbegriffe, wenn nur darin t statt r gesetzt wird.

Die übrigen Thatsachen und Beweise der Capitel XVII und XVIII lassen sich ebenfalls ohne Schwierigkeit umgestalten, und einige derselben erhalten bei Verwendung der neuen Begriffe sogar noch einen einfacheren Ausdruck.

Capitel XIX.

Die Bestimmung der Anzahl der Idealklassen des quadratischen Körpers.

§ 85.

Das Symbol $\left(\frac{a}{n}\right)$ für eine zusammengesetzte Zahl n.

Ein bemerkenswerter Ausdruck für die Anzahl h der Idealklassen des quadratischen Körpers k ergiebt sich aus der Formel des Satzes 109, wenn wir die rechter Hand stehende Grösse

$$\underset{s=1}{L}\ \underset{(p)}{\Pi}\frac{1}{1-\left(\frac{d}{p}\right)p^{-s}}$$

durch Rechnung in geschlossener Form auswerten. Zu dem Zwecke ist es nötig, das Symbol $\left(\frac{a}{n}\right)$ auch für den Fall zu definiren, dass n eine zusammengesetzte ganze rationale positive Zahl bedeutet. Ist $n = pq\ldots w$, wo $p, q, \ldots, w$ rationale gleiche oder verschiedene Primzahlen sind, so definiren wir:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)\cdots\left(\frac{a}{w}\right);$$

ferner soll $\left(\frac{a}{1}\right)$ stets $+1$ bedeuten. Dadurch wird für $s > 1$:

$$\underset{(p)}{\Pi}\frac{1}{1-\left(\frac{d}{p}\right)p^{-s}} = \sum_{(n)}\left(\frac{d}{n}\right)\frac{1}{n^s},$$

wo die Summe sich über alle ganzen rationalen positiven Zahlen n erstreckt. Die Berechnung des Grenzwertes dieser Summe für $s = 1$ führt zu einem geschlossenen Ausdruck für die Klassenanzahl h; wir sprechen das Resultat in dem jetzt folgenden Satze aus.

§ 86.

Der geschlossene Ausdruck für die Anzahl der Idealklassen.

Satz 114. Die Anzahl h der Idealklassen des Körpers $k(\sqrt{m})$ ist:

$$h = -\frac{w}{2|d|}\sum_{(n)}\left(\frac{d}{n}\right)n \qquad \text{für } m<0,$$

$$h = \frac{1}{2\log\varepsilon}\log\frac{\prod\limits_{(b)}\left(e^{\frac{bi\pi}{d}}-e^{-\frac{bi\pi}{d}}\right)}{\prod\limits_{(a)}\left(e^{\frac{ai\pi}{d}}-e^{-\frac{ai\pi}{d}}\right)} \qquad \text{für } m>1,$$

wo die Summe $\sum\limits_{(n)}$ über die $|d|$ ganzen rationalen Zahlen $n=1, 2, \ldots, |d|$, und wo die Producte $\prod\limits_{(a)}$, $\prod\limits_{(b)}$ über alle diejenigen Zahlen a oder b unter diesen $|d|$ Zahlen zu erstrecken sind, welche der Bedingung $\left(\frac{d}{a}\right)=+1$ bezüglich $\left(\frac{d}{b}\right)=-1$ genügen. [*Dirichlet*[8, 9], *Weber*[4].]

Beweis. Es seien n, n' Zahlen >0. Wenn n und d einen gemeinsamen Teiler $\neq\pm1$ besitzen, so ist $\left(\frac{d}{n}\right)=0$. Ist dagegen n prim zu d, so wird, wie man leicht einsieht, $\left(\frac{d}{n}\right)=\prod\limits_{(w)}\left(\frac{d, n}{w}\right)$, wo das Product über alle verschiedenen rationalen Primzahlen w zu erstrecken ist, die in n aufgehen. Nach Hülfssatz 14 stellt dann das Product $\prod\limits_{(l)}\left(\frac{d, n}{l}\right)$ die nämliche Einheit dar, wenn l alle in d aufgehenden Primzahlen durchläuft. Ist nun $n'\equiv n$ nach d, so wird:

$$\prod_{(l)}\left(\frac{d, n}{l}\right)=\prod_{(l)}\left(\frac{d, n'}{l}\right),$$

und mit Rücksicht hierauf erhalten wir:

$$\left(\frac{d}{n}\right)=\left(\frac{d}{n'}\right), \tag{29.}$$

wenn $n\equiv n'$ nach d ist.

Ferner ergiebt sich

$$\left(\frac{d}{1}\right)+\left(\frac{d}{2}\right)+\cdots+\left(\frac{d}{d}\right) = 0, \tag{30.}$$

indem wir eine Zahl b bestimmen, derart, dass $\left(\frac{d}{b}\right) = -1$ ist, und dann erwägen, dass die linke Seite von (30.) mit Rücksicht auf (29.) in die Gestalt

$$\left(\frac{d}{b}\right)+\left(\frac{d}{2b}\right)+\cdots+\left(\frac{d}{db}\right) = -\left\{\left(\frac{d}{1}\right)+\left(\frac{d}{2}\right)+\cdots+\left(\frac{d}{d}\right)\right\}$$

gesetzt werden kann.

Durch Benutzung der Formel

$$\frac{1}{n^s} = \frac{1}{\Gamma(s)}\int_0^\infty \mathrm{e}^{-nt}\, t^{s-1}\, \mathrm{d}t.$$

wird, wenn wir die Regel (29.) berücksichtigen:

$$\underset{s=1}{L} \sum_{(n)} \left(\frac{d}{n}\right)\frac{1}{n^s} = \underset{s=1}{L}\int_0^\infty \frac{F(\mathrm{e}^{-t})\, t^{s-1}}{1-\mathrm{e}^{-dt}}\, \mathrm{d}t,$$

wo zur Abkürzung

$$F(x) = \left(\frac{d}{1}\right)x+\left(\frac{d}{2}\right)x^2+\cdots+\left(\frac{d}{d}\right)x^d$$

gesetzt ist. Wegen der Gleichung (30.) enthält $F(x)$ den Factor $1-x$; die rationale Function $\frac{F(\mathrm{e}^{-t})}{1-\mathrm{e}^{-dt}}$ bleibt mithin für $t=0$ endlich. Aus diesem Grunde ist

$$\underset{s=1}{L}\int_0^\infty \frac{F(\mathrm{e}^{-t})\, t^{s-1}}{1-\mathrm{e}^{-dt}}\, \mathrm{d}t = \int_0^\infty \frac{F(\mathrm{e}^{-t})}{1-\mathrm{e}^{-dt}}\, \mathrm{d}t.$$

Wenn wir in dem letzteren Integral die neue Integrationsveränderliche $x = \mathrm{e}^{-t}$ einführen, so erhält dasselbe die Gestalt:

$$\int_0^1 \frac{F(x)}{x(1-x^d)}\, \mathrm{d}x.$$

Nun haben wir die Zerlegung in Partialbrüche:

$$\frac{F(x)}{x(1-x^d)} = -\frac{1}{d}\sum_{(n)} \frac{F\left(\mathrm{e}^{\frac{2ni\pi}{d}}\right)}{x-\mathrm{e}^{\frac{2ni\pi}{d}}},$$

wo die Summe über $n = 1, 2, \ldots, |d|$ zu erstrecken ist, und nach

einem Satze von *Gauss* wird $F(e^{\frac{2ni\pi}{d}})$, d. i.

$$\sum_{(n')}\left(\frac{d}{n'}\right)e^{\frac{2nn'i\pi}{d}}=\left(\frac{d}{n}\right)\sqrt{d};$$

n' durchläuft hier wiederum die Zahlen $1, 2, \ldots, |d|$ und $\sqrt{d}$ ist bei positivem d positiv, bei negativem d positiv imaginär zu nehmen (vgl. § 124). Da ferner

$$\int_0^1\frac{dx}{x-e^{\frac{2ni\pi}{d}}}=\log\frac{e^{\frac{ni\pi}{|d|}}-e^{-\frac{ni\pi}{|d|}}}{i}-\frac{i\pi}{|d|}(n-\tfrac{1}{2}d)$$

$$(n=1, 2, \ldots, |d|)$$

ist, wo für den Logarithmus der reelle Wert desselben zu nehmen ist, so folgt ohne Schwierigkeit das im Satze 114 angegebene Resultat.

Die Form dieses Resultates ist eine wesentlich verschiedene, je nachdem der Körper k imaginär oder reell ist. Im ersteren Falle kann h aus der angegebenen Formel ohne Weiteres berechnet werden. Im zweiten Falle ist zuvor die Kenntnis der Grundeinheit ε erforderlich; der Quotient der beiden Producte $\underset{(a)}{\Pi}$ und $\underset{(b)}{\Pi}$ ist, wie sich an einer späteren Stelle (vgl. § 121) zeigen wird, nichts anderes, als eine gewisse aus der Theorie der Kreisteilung für den quadratischen Körper k sich ergebende Einheit.

Um ein Beispiel für den Fall eines imaginären Körpers zu nehmen, so erhält man, wenn $m=-p$ ist und p eine rationale positive Primzahl $\equiv 3$ nach 4 und überdies >3 bedeutet:

$$h=\frac{\Sigma b-\Sigma a}{p};$$

hierin bezeichnen Σa, Σb bezüglich die Summe der quadratischen Reste und die Summe der quadratischen Nichtreste nach p, die zwischen 0 und p liegen. Durch eine leichte Umformung kann in dem obigen Ausdrucke für h der Nenner p beseitigt werden; dadurch ergiebt sich die Klassenanzahl h auch gleich dem Ueberschuss der Anzahl der zwischen 0 und $\frac{p}{2}$ liegenden quadratischen Reste von p über die Anzahl der zwischen denselben Grenzen liegenden quadratischen Nichtreste oder gleich dem dritten Teil dieses Ueberschusses, je nachdem $p\equiv 7$ oder $\equiv 3$ nach 8 ist. Die erstere Anzahl übertrifft also stets die letztere Anzahl, eine auf rein arithmetischem Wege bisher nicht bewiesene Thatsache.

§ 87.
Der Dirichlet'sche biquadratische Zahlkörper.

Eine nahe liegende Verallgemeinerung der bis hierher entwickelten Theorie des quadratischen Körpers betrifft folgendes Problem. Es werde statt des natürlichen aus allen rationalen Zahlen bestehenden Rationalitätsbereiches ein quadratischer Zahlkörper k als Rationalitätsbereich zu Grunde gelegt; dann sollen die in Bezug auf k relativ quadratischen Körper K untersucht werden, d. h. diejenigen biquadratischen Zahlkörper K, die den gegebenen Körper k als Unterkörper enthalten.

Wenn der Körper k durch die imaginäre Einheit $\sqrt{-1}$ bestimmt ist, so bezeichne ich K als einen **Dirichlet'schen biquadratischen Körper.** Für diesen Fall liegen umfassende Untersuchungen vor. [*Dirichlet*[10, 11, 12], *Eisenstein*[3, 6], *Bachmann*[1, 3], *Minnigerode*[1], *Hilbert*[4].] Nach der entsprechenden Einteilung der Idealklassen des Körpers K in Geschlechter und geeigneter Uebertragung der Bezeichnungen gilt auch hier wiederum der Fundamentalsatz 100, und es sind die beiden in Capitel XVIII angewandten Beweismethoden dieses Satzes auch auf den Körper K übertragbar, so dass jener Fundamentalsatz für den Dirichlet'schen biquadratischen Körper sowohl eine reine arithmetische Begründung [*Hilbert*[4]] als auch einen Beweis mittelst der transcendenten Dirichlet'schen Methode [*Dirichlet*[10, 11, 12], *Minnigerode*[1]] zulässt.

Von besonderem Interesse ist der Fall, dass der Dirichlet'sche biquadratische Körper K ausser dem quadratischen Körper $\sqrt{-1}$ noch zwei andere quadratische Körper $k(\sqrt{+m})$ und $k(\sqrt{-m})$ enthält. Für einen solchen **speciellen Dirichlet'schen Körper** K gilt die wiederum auf transcendentem und auch auf rein arithmetischem Wege zu beweisende Thatsache:

Satz 115. Die Anzahl der Idealklassen in einem speciellen Dirichlet'schen biquadratischen Körper $K(\sqrt{+m}, \sqrt{-m})$ ist gleich dem Product der Klassenanzahlen in den quadratischen Körpern $k(\sqrt{+m})$ und $k(\sqrt{-m})$ oder gleich der Hälfte dieses Productes, je nachdem für die Grundeinheit des Körpers K die Relativnorm in Bezug auf $k(\sqrt{-1})$ gleich $\pm i$ oder gleich ± 1 wird.

Dieses Resultat bezeichnet *Dirichlet* als einen der schönsten Sätze der Theorie der imaginären Zahlen und als überraschend, weil durch dasselbe ein Zusammenhang zwischen denjenigen quadratischen Körpern

aufgedeckt wird, die durch Quadratwurzeln aus entgegengesetzten reellen Zahlen bestimmt sind.

Bei dem rein arithmetischen Beweise dieses Satzes gelingt es zugleich in sehr einfacher Weise, und zwar durch bestimmte Bedingungen für die Geschlechtscharaktere, diejenigen Idealklassen des biquadratischen Körpers $K(\sqrt{+m}, \sqrt{-m})$ zu kennzeichnen, welche als Producte aus einer Idealklasse von $k(\sqrt{+m})$ und einer Idealklasse von $k(\sqrt{-m})$ erhalten werden können. [*Hilbert*[4].]

Capitel XX.

Die Zahlringe und Moduln des quadratischen Körpers.

§ 88.

Die Zahlringe des quadratischen Körpers.

Die Theorie der Ringe und Moduln eines quadratischen Körpers erledigt sich rasch durch Specialisirung der allgemeinen in Capitel IX entwickelten Sätze. Man findet leicht, dass jeder Ring r des Körpers k durch eine einzige Zahl von der Gestalt $\varrho = f\omega$ erzeugt werden kann, wo ω die in § 59 definirte Zahl bedeutet, die mit 1 zusammen eine Basis von k bildet, und wo f eine gewisse positive ganze rationale Zahl, nämlich den Führer des Ringes r, bezeichnet. Ist insbesondere d negativ und ausserdem < -4, so findet sich nach Satz 66 die Anzahl h_r der regulären Ringklassen des Ringes r durch die Formel

$$h_r = hf \prod_{(p)} \left(1 - \left(\frac{d}{p}\right)\frac{1}{p}\right)$$

ausgedrückt, wo das Product über alle in f enthaltenen von einander verschiedenen rationalen Primzahlen p zu erstrecken ist. [*Dedekind*[1, 3].]

§ 89.

Ein Satz von den Modulklassen des quadratischen Körpers. Die binären quadratischen Formen.

Betreffs der Modulklassen endlich gilt im quadratischen Körper die folgende Thatsache:

Satz 116. In einer beliebigen Modulklasse des quadratischen Körpers k giebt es stets reguläre Ringideale. [*Dedekind*[1].]

Beweis. Es sei $[\mu_1, \mu_2]$ ein beliebiger Modul des Körpers k, wobei also μ_1, μ_2 ganze Zahlen sind, und $\partial = f^2 d$ die Discriminante der durch $[\mu_1, \mu_2]$ bestimmten Modulklasse; ferner bezeichne $\mathfrak{m} = (\mu_1, \mu_2)$ das durch die Zahlen μ_1, μ_2 bestimmte Ideal und $s\mathfrak{m} = \mathfrak{m}'$ das zu $\mathfrak{m}$ conjugirte Ideal. Nunmehr bestimme man eine durch $\mathfrak{m}'$ teilbare ganze Zahl α des Körpers k so, dass $\frac{\alpha}{\mathfrak{m}'}$ prim zu ∂ ausfällt. Setzen wir dann

$$\alpha_1 = \frac{\alpha\mu_1}{n(\mathfrak{m})}, \quad \alpha_2 = \frac{\alpha\mu_2}{n(\mathfrak{m})},$$

so wird $[\alpha_1, \alpha_2]$ ein mit $[\mu_1, \mu_2]$ äquivalenter Modul, während zugleich das durch α_1, α_2 bestimmte Ideal $\mathfrak{a} = (\alpha_1, \alpha_2)$ prim zu ∂ ausfällt.

Ist nun ∂ eine gerade Zahl, so ziehen wir zunächst die drei ganzen Zahlen α_1, α_2, $\alpha_1 + \alpha_2$ in Betracht; darunter ist notwendig mindestens eine prim zu 2, denn anderenfalls müssten sich unter diesen drei Zahlen gewiss irgend zwei finden, die mit der Zahl 2 einen und den nämlichen idealen Primfactor gemein haben, was dem widerspräche, dass das Ideal $\mathfrak{a}$ prim zu ∂ ist. Es sei etwa α_1 prim zu 2. Nunmehr bezeichne man die ungeraden in ∂ aufgehenden rationalen Primzahlen mit p, q, $\ldots$, w. Da $\mathfrak{a}$ prim zu p ist, so muss mindestens eine der drei Zahlen α_1, $\alpha_1 + \alpha_2$, $\alpha_1 + 2\alpha_2$ prim zu p sein. Es sei $\alpha_1 + x\alpha_2$ prim zu p, ferner sei $\alpha_1 + y\alpha_2$ prim zu q, $\ldots$, wo x, y, $\ldots$ ganze rationale Zahlen bedeuten sollen. Dann folgt leicht die Existenz einer ganzen rationalen Zahl a von der Art, dass $\alpha_1 + a\alpha_2$ prim zu ∂ wird.

Setzen wir nun

$$b = \frac{|n(\alpha_1 + a\alpha_2)|}{n(\mathfrak{a})}, \quad \beta = \frac{\alpha_2(\alpha_1' + a\alpha_2')}{n(\mathfrak{a})},$$

wo α_1', α_2' die zu α_1, α_2 conjugirten Zahlen bedeuten, so ist b eine ganze rationale positive und β eine ganze algebraische Zahl, und es wird der Modul $[\alpha_1, \alpha_2] = [\alpha_1 + a\alpha_2, \alpha_2]$ äquivalent dem Modul $[b, \beta]$. Zugleich ergiebt sich wegen $(b, \beta) = \frac{\alpha_1' + a\alpha_2'}{\mathfrak{a}'}$ die Norm $n(b, \beta) = b$. Der Modul $[b, \beta]$ ist offenbar ein reguläres Ringideal in dem durch die Zahl β bestimmten Ringe $r = [\beta]$, und hiermit ist der Satz 116 vollständig bewiesen.

Wegen

$$\partial = \frac{1}{(n(b, \beta))^2} \begin{vmatrix} b, & \beta \\ b, & \beta' \end{vmatrix}^2 = \begin{vmatrix} 1, & \beta \\ 1, & \beta' \end{vmatrix}^2$$

stimmt die Discriminante dieses Ringes r mit der Discriminante der betrachteten Modulklasse überein. Der erhaltene Ring r ist zugleich der einzige, welcher mit $[\mu_1, \mu_2]$ äquivalente Moduln unter seinen regulären Ringidealen aufweist. Der Satz 116 zeigt, dass es im quadratischen Körper auf dasselbe hinauskommt, die Modulklassen oder die Klassen regulärer Ringideale zu betrachten.

Nach den allgemeinen Ausführungen in § 30 und § 35 entspricht einer jeden Modulklasse eines quadratischen Körpers $k(\sqrt{m})$ eine Klasse binärer quadratischer Formen mit ganzzahligen Coefficienten, und umgekehrt entspricht jeder solchen Formenklasse mit einer nichtquadratischen Discriminante eine Modulklasse eines quadratischen Körpers, wobei die Modulklasse und die Formen stets gleiche Discriminante besitzen. Danach ist durch die Untersuchungen in diesem Abschnitte zugleich die Theorie der quadratischen Formen mit vorgeschriebener Discriminante ∂ vollständig erledigt.

§ 90.

Die niedere und die höhere Theorie des quadratischen Zahlkörpers.

Die in diesem dritten Teile des Berichtes entwickelten und einheitlich dargestellten Untersuchungen machen die niedere Theorie des quadratischen Zahlkörpers aus; unter der höheren Theorie des quadratischen Zahlkörpers begreife ich die Darstellung derjenigen Eigenschaften dieses Körpers, zu deren naturgemässer Herleitung die Benutzung gewisser Hülfskörper höheren Grades nötig ist. Ein Abschnitt dieser höheren Theorie findet in dem vierten Teil dieses Berichtes Platz. Die Theorie der zu einem imaginären quadratischen Körper gehörigen Klassenkörper sowie der dazu gehörigen relativ-Abel'schen Körper erfordert jedoch zu ihrem Aufbau die Methode der complexen Multiplication der elliptischen Functionen, und dies ist ein Gegenstand, welcher von der Aufnahme in diesen Bericht ausgeschlossen werden musste.

Vierter Teil.

Der Kreiskörper.

Capitel XXI.

Die Einheitswurzeln mit Primzahlexponent l und der durch sie bestimmte Kreiskörper.

§ 91.

Der Grad des Kreiskörpers der $l$ten Einheitswurzeln und die Zerlegung der Primzahl l in diesem Körper.

Es bedeute l eine ungerade rationale Primzahl, und es sei $\zeta = e^{\frac{2i\pi}{l}}$. Die Gleichung $l$ten Grades

$$x^l - 1 = 0$$

besitzt die l Wurzeln

$$\zeta, \quad \zeta^2, \quad \ldots, \quad \zeta^{l-1}, \quad \zeta^l = 1.$$

Diese Zahlen heissen **die $l$ten Einheitswurzeln.** Der durch sie bestimmte Körper werde mit $k(\zeta)$ bezeichnet und der **Kreiskörper** der $l$ten Einheitswurzeln genannt. Es gilt für ihn zunächst die folgende Thatsache:

Satz 117. Bedeutet l eine ungerade Primzahl, so besitzt der durch $\zeta = e^{\frac{2i\pi}{l}}$ bestimmte Kreiskörper $k(\zeta)$ der $l$ten Einheitswurzeln den Grad $l-1$. Die Primzahl l gestattet in $k(\zeta)$ die Zerlegung $l = \mathfrak{l}^{l-1}$, wo $\mathfrak{l} = (1-\zeta)$ ein Primideal ersten Grades in $k(\zeta)$ ist.

Beweis. Die Zahl ζ genügt der Gleichung $l-1$ten Grades

$$F(x) = \frac{x^l - 1}{x - 1} = x^{l-1} + x^{l-2} + \cdots + 1 = 0;$$

also ist der Körper $k(\zeta)$ höchstens vom Grade $l-1$. Da $\zeta, \zeta^2, \ldots, \zeta^{l-1}$ die $l-1$ Wurzeln dieser Gleichung $F(x)=0$ sind, so gilt identisch in x die Gleichung:

$$x^{l-1}+x^{l-2}+\cdots+1 = (x-\zeta)(x-\zeta^2)\ldots(x-\zeta^{l-1});$$

für $x=1$ folgt hieraus:

$$(31.) \qquad l = (1-\zeta)(1-\zeta^2)\ldots(1-\zeta^{l-1}).$$

Es bedeute nun g eine beliebige durch l nicht teilbare ganze rationale Zahl >1, und es sei dann g' eine positive ganze rationale Zahl von der Art, dass $gg'\equiv 1$ nach l ausfällt. Dann sind die Quotienten

$$\frac{1-\zeta^g}{1-\zeta} = 1+\zeta+\zeta^2+\cdots+\zeta^{g-1}$$

und

$$\frac{1-\zeta}{1-\zeta^g} = \frac{1-\zeta^{gg'}}{1-\zeta^g} = \frac{1-(\zeta^g)^{g'}}{1-\zeta^g} = 1+\zeta^g+\zeta^{2g}+\cdots+\zeta^{(g'-1)g}$$

beide ganze algebraische Zahlen, und es erweist sich somit

$$\varepsilon_g = \frac{1-\zeta^g}{1-\zeta}$$

als eine Einheit des Körpers $k(\zeta)$. Setzen wir noch $\lambda = 1-\zeta$ und $\mathfrak{l}=(\lambda)$, so erhält die Formel (31.) die Gestalt

$$(32.) \qquad l = \lambda^{l-1}\varepsilon_2\varepsilon_3\ldots\varepsilon_{l-1} = \mathfrak{l}^{l-1}.$$

Aus Satz 33 schliesst man unmittelbar, dass eine rationale Primzahl in einem gegebenen Zahlkörper höchstens das Product so vieler Primideale sein kann, als der Grad des Körpers beträgt. In Anbetracht der Formel (32.) muss mithin der Grad des Körpers $k(\zeta)$ mindestens $=l-1$ sein, also ist nach dem bereits oben Gefundenen dieser Grad genau $=l-1$. Andererseits kann aus dem nämlichen Grunde das Ideal $\mathfrak{l}$ im Körper $k(\zeta)$ nicht noch weiter in Factoren zerfallen und es ist somit $\mathfrak{l}$ ein Primideal in $k(\zeta)$. [*Dedekind*[1].]

Das gewonnene Resultat besagt zugleich, dass die Function $F(x)$ im Bereich der rationalen Zahlen irreducibel ist.

§ 92.
Die Basis und die Discriminante des Kreiskörpers der $l$ten Einheitswurzeln.

Satz 118. In dem durch $\zeta = e^{\frac{2i\pi}{l}}$ bestimmten Kreiskörper $k(\zeta)$ der $l$ten Einheitswurzeln bilden die Zahlen

$$1, \quad \zeta, \quad \zeta^2, \quad \ldots, \quad \zeta^{l-2}$$

eine Basis. Die Discriminante des Kreiskörpers $k(\zeta)$ ist

$$d = (-1)^{\frac{l-1}{2}} l^{l-2}.$$

Beweis. Die Differente der Zahl ζ im Körper $k(\zeta)$ ist

$$\delta = (\zeta - \zeta^2)(\zeta - \zeta^3)\ldots(\zeta - \zeta^{l-1}) = \left[\frac{dF(x)}{dx}\right]_{x=\zeta}.$$

Aus

$$(x-1)F(x) = x^l - 1$$

folgt:

$$(x-1)\frac{dF(x)}{dx} + F(x) = l x^{l-1}, \quad \text{also} \quad \delta = -\frac{l\zeta^{l-1}}{1-\zeta};$$

nach der in § 3 (S. 180 oben) gemachten Bemerkung ist dann die Discriminante der Zahl ζ

$$d(\zeta) = (-1)^{\frac{(l-1)(l-2)}{2}} n(\delta) = (-1)^{\frac{l-1}{2}} l^{l-2}.$$

Da die Discriminante $d(\lambda)$ der Zahl λ offenbar den nämlichen Wert $d(\zeta)$ hat, so lehrt die im Beweise zu Satz 5 bei Formel (1.) S. 180 gemachte Bemerkung, dass eine jede ganze Zahl α des Körpers $k(\zeta)$ in der Gestalt

$$(33.) \qquad \alpha = \frac{a_0 + a_1\lambda + \cdots + a_{l-2}\lambda^{l-2}}{l^{l-2}}$$

mit ganzen rationalen Coefficienten $a_0, a_1, \ldots, a_{l-2}$ dargestellt werden kann.

Dabei müssen dann die Zahlen $a_0, a_1, \ldots, a_{l-2}$ notwendig sämtlich durch den Nenner l^{l-2} teilbar sein. Um zunächst zu zeigen, dass sie ein erstes Mal durch l teilbar sind, nehmen wir an, es fände sich unter ihnen etwa a_g als erster nicht durch l teilbarer Coefficient; aus $l^{l-2}\alpha \equiv 0$ nach l würde dann in Anbetracht von $l = \mathfrak{l}^{l-1}$ notwendig

$a_g \lambda^g \equiv 0$ nach $\mathfrak{l}^{g+1}$, d. h. $a_g \equiv 0$ nach $\mathfrak{l}$ und also auch nach l folgen, was der Annahme widerspricht. Man kann mithin einen Factor l in Zähler und Nenner des Ausdruckes (33.) fortheben. Durch die geeignete Weiterführung des eben angewandten Verfahrens folgt schliesslich, dass jede ganze Zahl α des Körpers $k(\zeta)$ bei ihren Darstellungen

$$\alpha = a_0 + a_1 \lambda + \cdots + a_{l-2} \lambda^{l-2} = b_0 + b_1 \zeta + \cdots + b_{l-2} \zeta^{l-2}$$

mit rationalen Coefficienten $a_0, a_1, \ldots, a_{l-2}$, bez. $b_0, b_1, \ldots, b_{l-2}$ für diese lauter ganze rationale Zahlen bekommt.

Da somit die Potenzen $1, \zeta, \ldots, \zeta^{l-2}$ der Zahl ζ eine Basis des Körpers $k(\zeta)$ bilden, so folgt, dass die Discriminante $d(\zeta)$ der Zahl ζ zugleich auch die Discriminante des Körpers $k(\zeta)$ vorstellt.

§ 93.

Die Zerlegung der von l verschiedenen rationalen Primzahlen im Kreiskörper der $l$ten Einheitswurzeln.

Die Zerlegung der Primzahl l im Körper $k(\zeta)$ ist in Satz 117 ausgeführt. Für die Zerlegungen der übrigen rationalen Primzahlen im Körper $k(\zeta)$ gilt die folgende Regel:

Satz 119. Ist p eine von l verschiedene rationale Primzahl und f der kleinste positive Exponent, für welchen $p^f \equiv 1$ nach l ausfällt, und wird dann $l-1 = ef$ gesetzt, so findet im Kreiskörper $k(\zeta)$ die Zerlegung

$$p = \mathfrak{p}_1 \cdots \mathfrak{p}_e$$

statt, wo $\mathfrak{p}_1, \ldots, \mathfrak{p}_e$ von einander verschiedene Primideale $f$ten Grades in $k(\zeta)$ sind. [*Kummer*[5, 6].]

Beweis. Es sei $\alpha = a + a_1 \zeta + \cdots + a_{l-2} \zeta^{l-2}$ eine beliebige ganze Zahl des Kreiskörpers $k(\zeta)$; dann folgen die Congruenzen

$$\alpha^p \equiv (a + a_1 \zeta + \cdots + a_{l-2} \zeta^{l-2})^p \equiv a + a_1 \zeta^p + \cdots + a_{l-2} \zeta^{p(l-2)}, \quad (p)$$

$$\alpha^{p^2} \equiv (a + a_1 \zeta^p + \cdots + a_{l-2} \zeta^{p(l-2)})^p \equiv a + a_1 \zeta^{p^2} + \cdots + a_{l-2} \zeta^{p^2(l-2)}, \quad (p)$$

. . . .

$$\alpha^{p^f} \equiv (a + a_1 \zeta^{p^{f-1}} + \cdots + a_{l-2} \zeta^{p^{f-1}(l-2)})^p \equiv a + a_1 \zeta^{p^f} + \cdots + a_{l-2} \zeta^{p^f(l-2)} \equiv \alpha, \ (p).$$

Ist nun $\mathfrak{p}$ ein in p aufgehendes Primideal, so folgt aus der eben erhaltenen Congruenz $\alpha^{p^f} \equiv \alpha$ nach p umsomehr $\alpha^{p^f} \equiv \alpha$ nach $\mathfrak{p}$, d. h. die Congruenz

$$(34.) \qquad \xi^{p^f} - \xi \equiv 0, \quad (\mathfrak{p})$$

wird von einer jeden ganzen Zahl des Körpers $k(\zeta)$ erfüllt. Die Anzahl der nach $\mathfrak{p}$ einander incongruenten Wurzeln dieser Congruenz (34.) ist daher gleich der Anzahl der vorhandenen nach $\mathfrak{p}$ incongruenten ganzen Zahlen, d. h. $= n(\mathfrak{p}) = p^{f'}$, wenn mit f' der Grad des Primideals p bezeichnet wird. Nun ist der Grad der Congruenz (34.) p^f; nach Satz 26 folgt daher $p^{f'} \leqq p^f$, d. h. $f' \leqq f$.

Andererseits ist nach Satz 24, dem verallgemeinerten Fermat'schen Satze, gewiss

$$(35.) \qquad \zeta^{p^{f'}-1} \equiv 1, \quad (\mathfrak{p}).$$

Da nach Formel (31.) für einen nicht durch l teilbaren Exponenten g die Zahl $1-\zeta^g$ stets zu $\mathfrak{p}$ prim ist, so folgt aus der Congruenz (35.): $p^{f'}-1 \equiv 0$ nach l, und damit $f' \geqq f$. Wir schliessen nunmehr $f' = f$, d. h. jedes in p aufgehende Primideal hat den Grad f.

Da p nicht in der Discriminante des Körpers $k(\zeta)$ aufgeht, so folgt nach Satz 31, dass p in lauter von einander verschiedene Primideale zerfällt. Setzen wir etwa $p = \mathfrak{p}_1 \dots \mathfrak{p}_{e'}$, so wird $n(p) = p^{l-1} = p^{e'f}$, d. h. $l-1 = e'f$, $e' = e$. Damit ist der Beweis des Satzes 119 vollständig erbracht.

Zur wirklichen Aufstellung der Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_e$ wenden wir den Satz 33 an und berücksichtigen die im Anschluss daran auf S. 202 gemachte Bemerkung. Danach gilt identisch in x nach p eine Zerlegung

$$F(x) \equiv F_1(x) \dots F_e(x), \quad (p),$$

wo $F_1(x), \dots, F_e(x)$ ganze nach p irreducible und einander incongruente Functionen vom $f$ten Grade in x mit ganzen rationalen Coefficienten bedeuten. Nach Bestimmung dieser Functionen erhalten wir die gewünschte Darstellung in den folgenden Formeln

$$\mathfrak{p}_1 = (p, F_1(\zeta)), \quad \dots, \quad \mathfrak{p}_e = (p, F_e(\zeta)).$$

Capitel XXII.

Die Einheitswurzeln für einen zusammengesetzten Wurzelexponenten m und der durch sie bestimmte Kreiskörper.

§ 94.

Der Kreiskörper der $m$ten Einheitswurzeln.

Es bedeute m eine beliebige positive ganze rationale Zahl, und es werde $Z = e^{\frac{2i\pi}{m}}$ gesetzt. Die Gleichung $m$ten Grades

$$x^m - 1 = 0$$

besitzt die m Wurzeln

$$Z, \quad Z^2, \quad \ldots, \quad Z^{m-1}, \quad Z^m = 1.$$

Diese Zahlen heissen **die $m$ten Einheitswurzeln;** der durch sie bestimmte Körper werde mit $k(Z)$ bezeichnet und der **Kreiskörper** der $m$ten Einheitswurzeln genannt.

Setzt man, falls m durch mehr als eine Primzahl teilbar ist:

$$m = l_1^{h_1} l_2^{h_2} \ \ldots,$$

wo $l_1, l_2, \ldots$ verschiedene rationale Primzahlen seien, so kann man eine Partialbruchzerlegung vornehmen

$$\frac{1}{m} = \frac{a_1}{l_1^{h_1}} + \frac{a_2}{l_2^{h_2}} + \cdots,$$

wo $a_1, a_2, \ldots$ ganze rationale positive oder negative Zahlen bedeuten, und dann a_1 zu l_1, a_2 zu $l_2, \ldots$ prim ist. Die Benutzung dieser Zerlegung liefert

$$Z = Z_1^{a_1} Z_2^{a_2} \ \ldots,$$

wenn $Z_1 = e^{\frac{2i\pi}{l_1^{h_1}}}$, $Z_2 = e^{\frac{2i\pi}{l_2^{h_2}}}$, $\ldots$ gesetzt wird; es entsteht also durch Zusammensetzung der Körper $k(Z_1)$ der $l_1^{h_1}$ten Einheitswurzeln, $k(Z_2)$ der $l_2^{h_2}$ten Einheitswurzeln, $\ldots$ genau der Rationalitätsbereich $k(Z)$. Wir behandeln dementsprechend zunächst den einfacheren Fall $m = l^h$, wo in m nur eine Primzahl l aufgeht.

§ 95.

Der Grad des Kreiskörpers der l^hten Einheitswurzeln und die Zerlegung der Primzahl l in diesem Körper.

Für den Kreiskörper der l^hten Einheitswurzeln gelten folgende Thatsachen:

Satz 120. Bedeutet l die Primzahl 2 oder eine ungerade Primzahl, so besitzt der durch $Z = e^{\frac{2i\pi}{l^h}}$ bestimmte Kreiskörper $k(Z)$ der l^hten Einheitswurzeln den Grad $l^{h-1}(l-1)$. Die Primzahl l gestattet in $k(Z)$ die Zerlegung $l = \mathfrak{L}^{l^{h-1}(l-1)}$, wo $\mathfrak{L}$ ein Primideal ersten Grades in $k(Z)$ ist.

Beweis. Z genügt der Gleichung vom $l^{h-1}(l-1)$ten Grade:

$$F(x) = \frac{x^{l^h}-1}{x^{l^{h-1}}-1} = x^{l^{h-1}(l-1)} + x^{l^{h-1}(l-2)} + \cdots + 1 = 0.$$

Bedeutet g eine nicht durch l teilbare ganze rationale Zahl und dann g' eine ganze rationale Zahl von der Art, dass $gg' \equiv 1$ nach l^h ausfällt, so folgt ähnlich wie auf S. 326, dass sowohl

$$E_g = \frac{1-Z^g}{1-Z},$$

als auch der reciproke Wert davon, nämlich:

$$\frac{1-Z}{1-Z^g} = \frac{1-Z^{gg'}}{1-Z^g}$$

ganze Zahlen sind; es ist daher E_g eine Einheit. Auf Grund dieses Umstandes können in der nämlichen Weise wie in § 91 die Gleichungen:

$$F(1) = l = \prod_{(g)}(1-Z^g) = \Lambda^{l^{h-1}(l-1)} \prod_{(g)} E_g = \mathfrak{L}^{l^{h-1}(l-1)}$$

geschlossen werden, wo $\Lambda = 1-Z$, $\mathfrak{L} = (\Lambda)$ gesetzt ist und in den Producten g alle zu l primen Zahlen > 0 und $< l^h$ zu durchlaufen hat.

Durch dieselbe Ueberlegung wie in § 91 folgt hieraus, dass der Grad des Körpers $k(Z)$ mindestens $= l^{h-1}(l-1)$ ist, und damit zugleich, dass er genau diesen Wert hat.

§ 96.
Die Basis und die Discriminante des Kreiskörpers der l^hten Einheitswurzeln.

Satz 121. In dem durch $Z = e^{\frac{2i\pi}{l^h}}$ bestimmten Kreiskörper $k(Z)$ der l^hten Einheitswurzeln bilden die Zahlen

$$1, \quad Z, \quad Z^2, \quad \ldots, \quad Z^{l^{h-1}(l-1)-1}$$

eine Basis; die Discriminante dieses Körpers ist

$$d = \pm l^{l^{h-1}(hl-h-1)},$$

wo für $l^h = 4$ und $l \equiv 3$ nach 4 das Vorzeichen — und sonst das Vorzeichen + gilt.

Satz 122. Ist p eine von l verschiedene rationale Primzahl und f der kleinste positive Exponent, für welchen $p^f \equiv 1$ nach l^h ausfällt, und wird $l^{h-1}(l-1) = ef$ gesetzt, so findet in $k(Z)$ die Zerlegung

$$p = \mathfrak{P}_1 \cdots \mathfrak{P}_e$$

statt, wo $\mathfrak{P}_1, \ldots, \mathfrak{P}_e$ von einander verschiedene Primideale $f$ten Grades in $k(Z)$ sind.

Die beiden Sätze 121 und 122 werden genau in der entsprechenden Weise bewiesen, wie die für den Körper $k(\zeta)$ aufgestellten Sätze 118 und 119.

§ 97.
Der Kreiskörper der $m$ten Einheitswurzeln. Der Grad, die Discriminante und die Primideale dieses Körpers.

Jetzt sei m ein Product aus Potenzen verschiedener Primzahlen, etwa $m = l_1^{h_1} l_2^{h_2} \ldots$. Der nach § 94 definirte Kreiskörper $k(Z)$ der $m$ten Einheitswuzeln entsteht dann, wie dort ausgeführt worden ist, durch Zusammensetzung der Kreiskörper $k(Z_1)$, $k(Z_2)$, ... der $l_1^{h_1}$ten, der $l_2^{h_2}$ten, ... Einheitswurzeln. Da die Discriminanten der letzteren Kreiskörper zu einander prim sind, so folgt aus Satz 87 (§ 52) unmittelbar die Thatsache:

Satz 123. Der Grad des Körpers $k(Z)$ der $m = l_1^{h_1} l_2^{h_2} \ldots$ten Einheitswurzeln ist:

$$\Phi(m) = l_1^{h_1-1}(l_1-1) l_2^{h_2-1}(l_2-1) \quad \ldots .$$

Wenden wir die zweite Aussage in Satz 88 auf die Kreiskörper $k(Z_1)$, $k(Z_2)$, ... an und beachten den Satz 121, so folgt das weitere Resultat:

Satz 124. Der Kreiskörper $k(Z)$ der $m$ten Einheitswurzeln besitzt die Basis:

$$1, \quad Z, \quad Z^2, \quad \ldots, \quad Z^{\Phi(m)-1}.$$

Die Discriminante des Körpers $k(Z)$ der $m$ten Einheitswurzeln ergiebt sich durch die erste Aussage in Satz 88.

Endlich kann auf Grund des Satzes 88 (vergl. die „Druckfehler, Berichtigungen und Zusätze" am Schlusse dieses Berichtes) unter Zuhülfenahme der Eigenschaften der Zerlegungs- und der Trägheitskörper die Zerlegung einer rationalen Primzahl p im Körper $k(Z)$ ausgeführt werden. Man erhält so den Satz:

Satz 125. Ist p eine in $m = l_1^{h_1} l_2^{h_2} \ldots$ nicht aufgehende rationale Primzahl und f der kleinste positive Exponent, für welchen $p^f \equiv 1$ nach m ausfällt, und wird dann $\Phi(m) = ef$ gesetzt, so findet im Kreiskörper $k(Z)$ der $m$ten Einheitswurzeln die Zerlegung

$$p = \mathfrak{P}_1 \ldots \mathfrak{P}_e$$

statt, wo $\mathfrak{P}_1, \ldots, \mathfrak{P}_e$ von einander verschiedene Primideale $f$ten Grades in $k(Z)$ sind.

Ist ferner p^h eine Potenz von p, und wird $m^* = p^h m$ gesetzt, so findet im Körper $k(Z^*)$ der m^*ten Einheitswurzeln die Zerlegung

$$p = \{\mathfrak{P}_1^* \ldots \mathfrak{P}_e^*\}^{p^{h-1}(p-1)}$$

statt, wo $\mathfrak{P}_1^*, \ldots, \mathfrak{P}_e^*$ von einander verschiedene Primideale $f$ten Grades in $k(Z^*)$ sind. [*Kummer*[15], *Dedekind*[5], *Weber*[4].]

Nach Satz 123 genügt $Z = e^{\frac{2i\pi}{m}}$ einer irreduciblen Gleichung $F(x) = 0$ vom $\Phi(m)$ten Grade mit ganzen rationalen Coefficienten, und nach dem Beweise zu Satz 87 bleibt diese Gleichung $F(x) = 0$ auch noch irreducibel, wenn man als Rationalitätsbereich irgend einen Körper zu Grunde legt, dessen Discriminante zu m prim ist. [*Kronecker*[3, 21]].

Die Bildung der linken Seite $F(x)$ dieser Gleichung geschieht in folgender Weise. Wird für den Augenblick zur Abkürzung allgemein

$$x^m - 1 = [m]$$

und

$$\Pi_0 = [m],$$
$$\Pi_1 = \left[\frac{m}{l_1}\right]\left[\frac{m}{l_2}\right]\ldots,$$
$$\Pi_2 = \left[\frac{m}{l_1 l_2}\right]\left[\frac{m}{l_1 l_3}\right]\ldots\left[\frac{m}{l_2 l_3}\right]\ldots,$$
$$\Pi_3 = \left[\frac{m}{l_1 l_2 l_3}\right]\left[\frac{m}{l_1 l_2 l_4}\right]\ldots\left[\frac{m}{l_2 l_3 l_4}\right]\ldots,$$
$$\cdots\cdots\cdots\cdots$$

gesetzt, so ist:

$$F(x) = \frac{\Pi_0 \Pi_2 \Pi_4 \ldots}{\Pi_1 \Pi_3 \Pi_5 \ldots}.$$

[*Dedekind*[1], *Bachmann*[2].]

Ist a eine ganze rationale Zahl und p eine in $F(a)$ aufgehende zu m prime Primzahl, so hat mit Rücksicht auf Satz 125 p stets die Congruenzeigenschaft $p \equiv 1$ nach m. Es giebt danach offenbar unendlich viele Primzahlen p mit dieser Congruenzeigenschaft.

§ 98.

Die Einheiten des Kreiskörpers $k(e^{\frac{2i\pi}{m}})$. Die Definition der Kreiseinheiten.

Es gelten folgende Thatsachen:

Satz 126. Wenn m eine Potenz einer Primzahl l ist und g eine nicht durch l teilbare Zahl bedeutet, so stellt in dem durch $Z = e^{\frac{2i\pi}{m}}$ bestimmten Kreiskörper der Ausdruck

$$\frac{1 - Z^g}{1 - Z}$$

stets eine Einheit dar.

Wenn die Zahl m verschiedene Primfactoren enthält und g eine zu m prime Zahl bedeutet, so stellt in dem durch $Z = e^{\frac{2i\pi}{m}}$ bestimmten Kreiskörper der Ausdruck

$$1 - Z^g$$

stets eine Einheit dar.

Beweis. Der erste Teil dieses Satzes 126 ist bereits in den Beweisen der Sätze 117 und 120 festgestellt worden. Um den zweiten

Teil zu beweisen, setzen wir $m = l_1^{h_1} l_2^{h_2} l_3^{h_3} \dots$ und

$$\frac{g}{m} = \frac{a}{l_1^{h_1}} + \frac{b}{l_2^{h_2} l_3^{h_3} \dots},$$

wo a eine zu l_1 und b eine zu $l_2, l_3, \dots$ prime ganze rationale Zahl bezeichnet; dabei wird

$$(36.) \qquad 1 - Z^g = 1 - e^{\frac{2i\pi g}{m}} = 1 - e^{\frac{2i\pi a}{l_1^{h_1}}} e^{\frac{2i\pi b}{l_2^{h_2} l_3^{h_3} \dots}}.$$

Nun ist:

$$\underset{(x)}{\Pi}\left(1 - e^{\frac{2i\pi x}{l_1^{h_1}}} e^{\frac{2i\pi b}{l_2^{h_2} l_3^{h_3} \dots}}\right) = 1 - e^{\frac{2i\pi b l_1^{h_1}}{l_2^{h_2} l_3^{h_3} \dots}},$$

wo das Product über $x = 0, 1, 2, \dots, l_1^{h_1} - 1$ zu erstrecken ist, oder:

$$(37.) \qquad \underset{(x')}{\Pi}\left(1 - e^{\frac{2i\pi x'}{l_1^{h_1}}} e^{\frac{2i\pi b}{l_2^{h_2} l_3^{h_3} \dots}}\right) = \frac{1 - e^{\frac{2i\pi b l_1^{h_1}}{l_2^{h_2} l_3^{h_3} \dots}}}{1 - e^{\frac{2i\pi b}{l_2^{h_2} l_3^{h_3} \dots}}},$$

wo das Product über $x' = 1, 2, \dots, l_1^{h_1} - 1$ zu erstrecken ist.

Wir unterscheiden jetzt zwei Fälle, je nachdem die Anzahl der Primzahlen $l_1, l_2, \dots$, die in m enthalten sind, zwei oder mehr als zwei beträgt. Im ersteren Falle ist die rechte Seite der Formel (37.) nach dem bereits feststehenden ersten Teile des Satzes 126 eine Einheit. Im zweiten Falle können wir annehmen, der zu beweisende Satz 126 sei bereits für diejenigen Kreiskörper $k(e^{\frac{2i\pi}{m^*}})$ als richtig erkannt, bei welchen die Zahl m^* durch weniger Primzahlen als m teilbar ist; es trifft dann dieser Satz für den Kreiskörper zu, der durch die $\frac{m}{l_1^{h_1}}$ ten Einheitswurzeln bestimmt ist. Danach sind dann Zähler und Nenner des auf der rechten Seite von (37.) stehenden Bruches für sich Einheiten. Der Ausdruck (36.) ist ein Factor des Productes auf der linken Seite von (37.) und daher gleichfalls in jedem Falle eine Einheit. Damit ist der Satz 126 vollständig bewiesen.

Von einer jeden beliebigen Einheit eines Kreiskörpers $k(e^{\frac{2i\pi}{m}})$ gilt die Thatsache, dass sie gleich dem Producte aus einer Einheitswurzel und einer reellen Einheit ist. Die Einheitswurzel liegt dabei nicht notwendig

immer in dem Körper $k(e^{\frac{2i\pi}{m}})$ selbst, sondern kann, wenn m verschiedene Primzahlen enthält, bei geradem m eine $2m$te, bei ungeradem m eine $4m$te Einheitswurzel sein. [*Kronecker*[7].] Wir sprechen insbesondere die folgende, schon von *Kummer* erkannte Thatsache aus:

Satz 127. Bezeichnet l eine ungerade Primzahl, und betrachten wir in dem durch $\zeta = e^{\frac{2i\pi}{l}}$ bestimmten Kreiskörper $k(\zeta)$ den durch $\zeta+\zeta^{-1}$ bestimmten reellen Unterkörper $k(\zeta+\zeta^{-1})$ vom Grade $\frac{l-1}{2}$, so ist ein beliebiges System von Grundeinheiten dieses reellen Körpers $k(\zeta+\zeta^{-1})$ stets auch für den Körper $k(\zeta)$ ein System von Grundeinheiten.

Beweis. Ist $\varepsilon(\zeta)$ eine beliebige Einheit in $k(\zeta)$, so ist $\frac{\varepsilon(\zeta)}{\varepsilon(\zeta^{-1})}$ eine solche Einheit in $k(\zeta)$, die selbst und deren Conjugirte sämtlich den absoluten Betrag 1 besitzen, und sie stellt daher nach Satz 48 eine Einheitswurzel dar; wir setzen $\frac{\varepsilon(\zeta)}{\varepsilon(\zeta^{-1})} \doteq \pm\zeta^{2g}$, wo g eine ganze Zahl sei. Die Einheit $\eta(\zeta) = \varepsilon(\zeta)\zeta^{-g}$ besitzt dann die Eigenschaft:

$$(38.) \qquad \frac{\eta(\zeta)}{\eta(\zeta^{-1})} = \pm 1.$$

In dieser Formel (38.) kann rechter Hand nur das positive Vorzeichen gelten. Anderenfalls nämlich wäre $\eta(\zeta)$ eine rein imaginäre Einheit; dann setzen wir $\eta^2 = \vartheta$, so dass ϑ eine Einheit des reellen Unterkörpers $k(\zeta+\zeta^{-1})$ wird. Die Relativdifferente der Zahl $\eta = \sqrt{\vartheta}$ in Bezug auf den reellen Unterkörper $k(\zeta+\zeta^{-1})$ ist 2η und mithin prim zu l. Demnach müsste auch die Relativdifferente des Körpers $k(\zeta)$ in Bezug auf den Körper $k(\zeta+\zeta^{-1})$ prim zu l sein. Bedeutet nun $\mathfrak{l}^*$ ein beliebiges in l aufgehendes Primideal des reellen Körpers $k(\zeta+\zeta^{-1})$, so würde daher nach Satz 93 dieses Ideal nicht gleich dem Quadrate eines Primideals des Körpers $k(\zeta)$ sein. Da aber $\mathfrak{l}^*$ in l höchstens zur $\frac{l-1}{2}$ten Potenz vorkommt, so fände sich diese letzte Folgerung in Widerspruch mit dem Satze 117 über die Zerlegung der Zahl l im Körper $k(\zeta)$; also gilt in der That auf der rechten Seite der Formel (38.) das obere Vorzeichen. Aus $\eta(\zeta) = \eta(\zeta^{-1})$ folgt, dass die Zahl $\eta(\zeta)$ reell ist. Damit ist der Beweis des Satzes 127 erbracht.

Die in Satz 126 angegebenen Einheiten sind imaginär. Um reelle

Einheiten zu erhalten, bilden wir, je nachdem m eine Potenz einer Primzahl ist oder verschiedene Primzahlen enthält, die Ausdrücke:

$$E_g = \sqrt{\frac{(1-Z^g)(1-Z^{-g})}{(1-Z\ )(1-Z^{-1})}}$$

bez.

$$E_g = \sqrt{(1-Z^g)(1-Z^{-g})},$$

wo g eine zu m prime Zahl bedeute und der positive Wert der Quadratwurzel genommen werde. Diese Einheiten sollen kurz **Kreiseinheiten** genannt werden. Mit Rücksicht auf $1-Z^{-g}=-Z^{-g}(1-Z^g)$ erkennt man, dass in dem ersteren Falle diese Einheiten im Körper $k(Z)$ selbst liegen, während sie im zweiten Falle als Producte aus Einheiten des Körpers $k(Z)$ in $2m$te bez. $4m$te Einheitswurzeln erscheinen, je nachdem m gerade oder ungerade ist.

Capitel XXIII.

Der Kreiskörper in seiner Eigenschaft als Abel'scher Körper.

§ 99.

Die Gruppe des Kreiskörpers der mten Einheitswurzeln.

Der Kreiskörper der $m$ten Einheitswurzeln ist bei jedem Werte von m, wie man leicht erkennt, ein Abel'scher Körper, und zwar gelten die folgenden eingehenderen Sätze:

Satz 128. Bedeutet l eine ungerade Primzahl, so ist der durch $Z=e^{\frac{2i\pi}{l^h}}$ bestimmte Kreiskörper ein cyklischer Körper.

Der durch $Z=e^{\frac{i\pi}{2^h}}$ $(h\geqq 2)$ bestimmte Kreiskörper entsteht durch Zusammensetzung des imaginären quadratischen Körpers $k(i)$ und des reellen Körpers $k\left(e^{\frac{i\pi}{2^h}}+e^{-\frac{i\pi}{2^h}}\right)$. Der reelle Körper $k\left(e^{\frac{i\pi}{2^h}}+e^{-\frac{i\pi}{2^h}}\right)$ ist cyklisch vom Grade 2^{h-1}.

Beweis. Der erste Teil des Satzes 128 folgt, wenn wir die Substitution

$$s = (Z : Z^r)$$

(Ersetzung von Z durch Z^r) einführen, wo unter r eine Primitivzahl nach l^h verstanden werden soll. Offenbar sind dann alle Substitutionen der Gruppe des Körpers $k(Z)$ Potenzen von s.

Um den zweiten Teil des Satzes 128 zu beweisen, betrachten wir die Substitutionen

$$s = (Z : Z^5), \quad s' = (Z : Z^{-1}) = (i : -i).$$

Dann folgt leicht, dass die Potenzen von s und deren Producte mit s' die sämtlichen Substitutionen des Körpers $k(Z)$ ausmachen.

Auf Grund des Satzes 128 ist auch für jede zusammengesetzte Zahl m die Gruppe des Kreiskörpers der $m$ten Einheitswurzeln unmittelbar anzugeben.

Die Aufstellung des Zerlegungs-, des Trägheits- und des Verzweigungskörpers für ein gegebenes Primideal in $k\left(e^{\frac{2i\pi}{m}}\right)$ kann auf Grund der Bedeutung dieser Unterkörper mit Hülfe der in § 95, § 96 und § 97 bewiesenen Sätze über die Zerlegung einer rationalen Primzahl im Kreiskörper leicht bewirkt werden. So ergiebt sich insbesondere das folgende Resultat:

Satz 129. Bedeutet l eine ungerade Primzahl, und betrachtet man den Kreiskörper $k(Z)$ der l^hten Einheitswurzeln, so ist für das in l enthaltene Primideal $\mathfrak{L} = (1 - Z)$ der Körper $k(Z)$ selbst der Verzweigungskörper, während der Körper der rationalen Zahlen gleichzeitig die Rolle des Zerlegungs- und des Trägheits-Körpers für $\mathfrak{L}$ übernimmt. Ist ferner $\mathfrak{P}$ ein von $\mathfrak{L}$ verschiedenes Primideal in $k(Z)$ vom Grade f, so ist für $\mathfrak{P}$ der Körper $k(Z)$ selbst der Trägheitskörper, während als Zerlegungskörper von $\mathfrak{P}$ derjenige Unterkörper $e = \frac{l^{h-1}(l-1)}{f}$ ten Grades von $k(Z)$ erscheint, der zu der Substitutionengruppe

$$s^e, \quad s^{2e}, \quad s^{3e}, \quad \ldots, \quad s^{fe}$$

gehört. Dabei bedeutet $s = (Z : Z^r)$ eine solche Substitution der Gruppe des Körpers $k(Z)$, welche mit ihren Potenzen diese Gruppe vollständig erzeugt.

§ 100.
Der allgemeine Begriff des Kreiskörpers. Der Fundamentalsatz über die Abel'schen Körper.

Wir erweitern nunmehr den Begriff des Kreiskörpers, wie er bisher in Betracht kam; wir bezeichnen als einen **Kreiskörper** schlechthin nicht nur einen jeden durch die Einheitswurzeln von irgend einem Exponenten m bestimmten Körper $k\left(e^{\frac{2i\pi}{m}}\right)$, sondern auch einen jeden, irgendwie in einem solchen besonderen Kreiskörper $k\left(e^{\frac{2i\pi}{m}}\right)$ enthaltenen Unterkörper. Da jeder Körper $k\left(e^{\frac{2i\pi}{m}}\right)$ ein Abel'scher Körper ist und ferner, wenn m und m' irgend welche Exponenten bedeuten, der Körper der $m$ten Einheitswurzeln und der Körper der m'ten Einheitswurzeln beide zugleich in dem Körper der $m.m'$ten Einheitswurzeln als Unterkörper enthalten sind, so gelten für diesen erweiterten Begriff des Kreiskörpers allgemein die folgenden Thatsachen:

Satz 130. Jeder Kreiskörper ist ein Abel'scher Körper. Jeder Unterkörper eines Kreiskörpers ist ein Kreiskörper. Jeder aus Kreiskörpern zusammengesetzte Körper ist wiederum ein Kreiskörper.

Es ist nun eine fundamentale Thatsache, dass die erste Aussage in diesem Satze 130 sich, wie folgt, umkehren lässt:

Satz 131. *Jeder Abel'sche Zahlkörper im Bereiche der rationalen Zahlen ist ein Kreiskörper.* [*Kronecker*[2,13], *Weber*[1], *Hilbert*[5].]

Um den Beweis dieses fundamentalen Satzes vorzubereiten, erinnern wir daran, dass nach § 48 jeder Abel'sche Körper sich aus solchen cyklischen Körpern zusammensetzen lässt, bei denen die Grade Primzahlen oder Primzahlpotenzen sind. Wir construiren nun folgende besonderen cyklischen Körper. Es bedeute u eine ungerade Primzahl und u^h eine Potenz derselben mit positivem Exponenten; dann ist der durch $e^{\frac{2i\pi}{u^{h+1}}}$ bestimmte Körper $k\left(e^{\frac{2i\pi}{u^{h+1}}}\right)$ ein cyklischer Körper vom $u^h(u-1)$ten Grade. Der cyklische Unterkörper vom u^hten Grade dieses Körpers werde mit U_h bezeichnet. Ferner bestimmt die Zahl $e^{\frac{i\pi}{2^{h+1}}}+e^{\frac{-i\pi}{2^{h+1}}}$ einen reellen cyklischen Körper vom 2^hten Grade. Dieser Körper werde mit II_h bezeichnet. Endlich sei l^h eine Potenz einer beliebigen Primzahl $l(=2$ oder $\neq 2)$ und ausserdem p eine Primzahl mit der Congruenz-

eigenschaft $p \equiv 1$ nach l^h; dann besitzt der Kreiskörper $k\left(e^{\frac{2i\pi}{p}}\right)$ vom Grade $p-1$ offenbar einen cyklischen Unterkörper vom Grade l^h. Dieser cyklische Körper l^hten Grades werde mit P_h bezeichnet. Die Körper U_h, II_h, P_h sind Kreiskörper bez. von den Graden u^h, 2^h, l^h; die Discriminanten dieser Körper U_h, II_h, P_h sind infolge der Sätze 39 und 121 Potenzen bez. der Primzahlen u, 2, p. Dass es bei jeder Annahme von l^h Primzahlen p mit der Congruenzeigenschaft $p \equiv 1$ nach l^h giebt, steht nach der letzten Bemerkung in § 97 fest, kommt jedoch hier nicht in Frage.

Wir werden in den folgenden Paragraphen zeigen, dass jeder Abelsche Körper als Unterkörper in einem solchen Körper enthalten ist, der durch Zusammensetzung aus $k(i)$ und geeigneten Körpern U_h, II_h, P_h entsteht. Zu diesem Nachweise ist eine Reihe von Hülfsbetrachtungen vorauszuschicken.

§ 101.

Ein allgemeiner Hülfssatz über cyklische Körper.

Hülfssatz 15. Wenn ein cyklischer Körper C_h von einem Grade l^h, wo l eine beliebige Primzahl ($=2$ oder $\neq 2$) ist, nicht den betreffenden Körper U_1 bez. II_1 als Unterkörper enthält, so entsteht durch Zusammensetzung von C_h mit dem durch $Z = e^{\frac{2i\pi}{l^h}}$ bestimmten Körper $k(Z)$ ein Körper $k(Z, C_h)$ vom Grade $l^{2h-1}(l-1)$, und es giebt dann stets in $k(Z)$ eine ganze Zahl $\varkappa$ mit folgenden Eigenschaften: der Körper $k(Z, C_h)$ ist auch durch die Zahlen Z und $\sqrt[l^h]{\varkappa}$ bestimmt; bezeichnet r eine beliebige nicht durch l teilbare ganze rationale Zahl, und wird aus der Gruppe des Körpers $k(Z)$ die Substitution

$$s = (Z : Z^r)$$

ins Auge gefasst, so ist $\varkappa^{s-r}$ die l^hte Potenz einer Zahl in $k(Z)$.

Beweis. Die erste Behauptung über den Grad von $k(Z, C_h)$ folgt unmittelbar daraus, dass $k(Z)$ und C_h ausser dem Körper der rationalen Zahlen keinen gemeinsamen Unterkörper haben. Es sei nun α eine den Körper C_h bestimmende ganze Zahl von der Art, dass auch keine Potenz von α in einem Unterkörper von C_h liegt; es sei ferner t eine solche Sub-

stitution der Gruppe von C_h, welche mit ihren Potenzen diese Gruppe erzeugt. Wir setzen, wenn a und b beliebige Exponenten sind:

$$K(\alpha^a, Z^b) = \alpha^a + Z^b.(t\alpha)^a + Z^{2b}.(t^2\alpha)^a + \cdots + Z^{(l^h-1)b}.(t^{l^h-1}\alpha)^a.$$

Die Ausdrücke $K(\alpha, Z)$, $K(\alpha^2, Z)$, ..., $K(\alpha^{l^h-1}, Z)$ können nicht sämtlich verschwinden, da sonst wegen $K(\alpha^0, Z) = 0$ notwendig auch die Determinante

$$\begin{vmatrix} 1, & 1, & \ldots, & 1 \\ \alpha, & t\alpha, & \ldots, & t^{l^h-1}\alpha \\ \cdot & \cdot & \cdot & \cdot \\ \alpha^{l^h-1}, & (t\alpha)^{l^h-1}, & \ldots, & (t^{l^h-1}\alpha)^{l^h-1} \end{vmatrix}$$

verschwinden müsste und dann nach der Bemerkung auf S. 180 die Zahl α keine den Körper C_h bestimmende Zahl wäre. Es sei $\alpha^* = \alpha^a$ eine solche Potenz von α, für welche $K = K(\alpha^*, Z) \neq 0$ ausfällt. Vermöge $K(t\alpha^*, Z^b) = Z^{-b} K(\alpha^*, Z^b)$ folgt dann, dass die Zahl K^{l^h} und ferner alle Zahlen $\dfrac{K(\alpha^*, Z^b)}{K^b}$ Zahlen in dem Körper $k(Z)$ sind. Da

$$\alpha^* = \frac{1}{l^h}\{K(\alpha^*, Z) + K(\alpha^*, Z^2) + \cdots + K(\alpha^*, Z^{l^h})\}$$

wird und α^* ebenfalls eine den Körper C_h bestimmende Zahl ist, so sehen wir, dass der durch K und Z bestimmte Körper, dessen Grad höchstens $l^{2h-1}(l-1)$ ist, den Körper $k(Z, C_h)$ vom Grade $l^{2h-1}(l-1)$ enthält; der erstere Körper ist daher mit diesem letzteren Körper identisch, und die Zahl $\varkappa = K^{l^h}$ besitzt die im Hülfssatze 15 angegebene Eigenschaft.

Wir machen noch folgende Bemerkung. Der durch Z und $\sqrt[l^h]{\varkappa}$ bestimmte Körper ist, wie man leicht erkennt, relativ cyklisch vom Relativgrade l^h in Bezug auf $k(Z)$ und besitzt daher einen einzigen Unterkörper, der $k(Z)$ enthält und relativ cyklisch vom Grade l in Bezug auf $k(Z)$ ist. Bedeutet nun C_1 den Unterkörper $l$ten Grades von C_h, so muss danach der aus $k(Z)$ und C_1 zusammengesetzte Körper mit dem durch Z und $\sqrt[l]{\varkappa}$ bestimmten Körper identisch sein.

§ 102.
Von gewissen Primzahlen in der Discriminante eines cyklischen Körpers vom Grade l^h.

Hülfssatz 16. Wenn C_h ein cyklischer Körper von einem Grade l^h ist, wo l eine beliebige Primzahl ($=2$ oder $\neq 2$) ist, und wenn C_1 den Unterkörper $l$ten Grades von C_h bezeichnet, so besitzen die etwaigen von l verschiedenen Primteiler p der Discriminante von C_1 durchweg die Congruenzeigenschaft $p \equiv 1$ nach l^h.

Beweis. Zunächst betrachten wir den Fall, dass l eine ungerade Primzahl und $h=1$ ist. Wir nehmen an, es fände sich im Gegensatz zu unserer Behauptung eine rationale, in der Discriminante von C_1 aufgehende Primzahl p, welche $\not\equiv 1$ nach l ist. Es sei $\zeta = e^{\frac{2i\pi}{l}}$, ferner r eine Primitivzahl nach l, und man nehme aus der Gruppe des Körpers $k(\zeta)$ die Substitution $s = (\zeta : \zeta^r)$. Ist $\mathfrak{p}$ ein idealer Primfactor von p im Körper $k(\zeta)$, so ist das Primideal $\mathfrak{p}$, wegen $p \not\equiv 1$ nach l, nach Satz 119 von einem Grade $f>1$; mithin ist nach Satz 129 der Zerlegungskörper des Primideals $\mathfrak{p}$ von einem Grade $e<l-1$; die übrigen Primfactoren von p sind dann

$$\mathfrak{p}' = s\mathfrak{p}, \quad \ldots, \quad \mathfrak{p}^{(e-1)} = s^{e-1}\mathfrak{p},$$

während $s^e\mathfrak{p} = \mathfrak{p}$, d. h.

$$(39.) \qquad \mathfrak{p}^{s^e-1} = 1$$

wird. Desgleichen gelten auch für die zu $\mathfrak{p}$ conjugirten Primideale $\mathfrak{p}'$, $\mathfrak{p}''$, ... die entsprechenden Gleichungen

$$(40.) \qquad \mathfrak{p}'^{s^e-1} = 1, \quad \mathfrak{p}''^{s^e-1} = 1, \quad \ldots.$$

Nach Hülfssatz 15 giebt es eine ganze Zahl $\varkappa$ in $k(\zeta)$, so dass die beiden Zahlen ζ und $\sqrt[l]{\varkappa}$ den aus $k(\zeta)$ und C_1 zusammengesetzten Körper $k(\zeta, C_1)$ bestimmen, und für welche obenein $\varkappa^{s-r}$ gleich der $l$ten Potenz einer Zahl in $k(\zeta)$ wird. Da $s-r$ und s^e-1 zwei ganzzahlige Functionen von s sind, welche im Sinne der Congruenz nach l keinen gemeinsamen Factor haben, so giebt es drei ganzzahlige Functionen $\varphi(s)$, $\psi(s)$, $\chi(s)$ der Veränderlichen s, so dass

$$1 = (s^e-1)\varphi(s) + (s-r)\psi(s) + l\chi(s)$$

ist, und hieraus folgt

$$\varkappa = \varkappa^{(s^e-1)\varphi(s)+(s-r)\psi(s)+l\chi(s)} = \varkappa^{(s^e-1)\varphi(s)}\alpha^l,$$

wo α eine Zahl in $k(\zeta)$ ist. Wegen der vorhin bewiesenen Gleichungen (39.) und (40.) für die Primideale $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \ldots$ lässt sich $\varkappa^{s^e-1}$ als eine solche ganze oder gebrochene Zahl schreiben, dass Zähler und Nenner keinen der Primfactoren $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \ldots$ enthalten und daher zu p prim sind; das Gleiche gilt somit von der Zahl $\varkappa^{(s^e-1)\varphi(s)}$. Wir setzen $\varkappa^{(s^e-1)\varphi(s)} = \frac{\varrho}{a^l}$ in solcher Weise, dass ϱ eine ganze, zu p prime Zahl in $k(\zeta)$ und a eine ganze rationale Zahl bedeutet. Der Körper $k(\zeta, C_1)$ wird dann auch durch die beiden Zahlen ζ und $\sqrt[l]{\varrho}$ bestimmt. Die Relativdiscriminante der Zahl $\sqrt[l]{\varrho}$ in Bezug auf $k(\zeta)$ ist $= \pm l^l \varrho^{l-1}$, und da ϱ zu p prim ist, so ist mithin auch die Relativdiscriminante von $k(\zeta, C_1)$ in Bezug auf $k(\zeta)$ prim zu p. Da andererseits auch die Discriminante von $k(\zeta)$ nicht durch p teilbar ist, so ist nach Satz 39 auch die Discriminante von $k(\zeta, C_1)$ und folglich nach Satz 85 auch die Discriminante des Körpers C_1 prim zu p, was unserer Annahme widerspricht.

In ähnlicher Weise erschliessen wir die Richtigkeit des Hülfssatzes 16 bei ungeradem l, wenn der Exponent $h > 1$ angenommen wird. Es sei $Z = e^{\frac{2i\pi}{l^h}}$, ferner bezeichne r eine Primitivzahl nach l^h, und aus der Gruppe des Körpers $k(Z)$ sei $s = (Z:Z^r)$. Es sei p eine in der Discriminante von C_1 aufgehende, von l verschiedene Primzahl und $\mathfrak{p}$ ein idealer Primfactor von p in $k(Z)$. Nehmen wir $p \equiv 1$ nach l, aber $\not\equiv 1$ nach l^h an, so liegt das Primideal $\mathfrak{p}$ jedenfalls auch in dem Unterkörper $k(Z^l)$ des Körpers $k(Z)$, d. h. es ist $\mathfrak{p}^{s^{l^{h-2}(l-1)}-1} = 1$, und ebenso gelten für die zu $\mathfrak{p}$ in $k(Z)$ conjugirten Primideale $\mathfrak{p}', \mathfrak{p}'', \ldots$ die Gleichungen:

$$\mathfrak{p}'^{s^{l^{h-2}(l-1)}-1} = 1, \quad \mathfrak{p}''^{s^{l^{h-2}(l-1)}-1} = 1, \quad \ldots .$$

Da r Primitivzahl nach l^h ist, so wird $r^{l^{h-2}(l-1)} \not\equiv 1$ nach l^h, und mithin lassen sich drei ganzzahlige Functionen $\varphi(s)$, $\psi(s)$, $\chi(s)$ der Variabeln s derart bestimmen, dass

$$l^{h-1} = (s^{l^{h-2}(l-1)}-1)\varphi(s) + (s-r)\psi(s) + l^h\chi(s)$$

ist; hieraus folgt alsdann, wenn $\varkappa$ eine nach Hülfssatz 15 bestimmte Zahl

bedeutet,

$$\varkappa^{l^{h-1}} = \varkappa^{(s^{l^{h-2}(l-1)}-1)\varphi(s)} \alpha^{l^h},$$

wo α eine Zahl in $k(Z)$ ist. Wegen der vorhin bewiesenen Eigenschaft der Primideale $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}'', \ldots$ ist $\varkappa^{s^{l^{h-2}(l-1)}-1}$ und folglich auch $\varkappa^{(s^{l^{h-2}(l-1)}-1)\varphi(s)}$ eine Zahl, deren Zähler und Nenner zu p prim ausfallen. Wir können daher die letztere Zahl $= \frac{\varrho}{a^{l^h}}$ setzen in solcher Weise, dass ϱ eine ganze, zu p prime Zahl in $k(Z)$ und a eine ganze rationale Zahl bedeutet. Es ist dann $\sqrt[l]{\varkappa} = \frac{\alpha}{a}\sqrt[l^h]{\varrho}$, und daraus ergiebt sich $\varrho = \sigma^{l^{h-1}}$, wo σ ebenfalls in $k(Z)$ liegt. Da der durch Z und $\sqrt[l]{\varkappa}$ bestimmte Körper, wie am Schlusse des § 101 bemerkt wurde, mit demjenigen Körper identisch ist, welcher durch Zusammensetzung aus $k(Z)$ und C_1 entsteht, und da die Relativdiscriminante der Zahl $\sqrt[l]{\sigma}$ in Bezug auf $k(Z)$ den zu p primen Wert $\pm l^l \sigma^{l-1}$ besitzt, so ist die Relativdiscriminante des Körpers $k(Z, C_1)$ in Bezug auf $k(Z)$ prim zu p. Andererseits ist die Discriminante von $k(Z)$ ebenfalls nicht durch p teilbar, und folglich gilt das Gleiche auch von der Discriminante des Körpers $k(Z, C_1)$ und damit dann auch von der des Körpers C_1. Der letztere Umstand aber widerspricht unserer Annahme.

Um die Richtigkeit des Hülfssatzes 16 für $l = 2$ zu erkennen, machen wir zunächst die Annahme $h = 2$ und wenden dann auf den cyklischen Körper C_2 vom 4ten Grade den Hülfssatz 15 an. Wir setzen $Z = e^{\frac{i\pi}{2}} = i$ und betrachten aus der Gruppe von $k(Z)$ die Substitution $s' = (i : -i)$. Es sei C_1 der quadratische Unterkörper von C_2, und wir nehmen an, es gebe eine in der Discriminante von C_1 aufgehende ungerade Primzahl p, welche $\not\equiv 1$ nach 4 ist. Infolge der letzteren Eigenschaft ist p in $k(i)$ unzerlegbar. Ist nun die uns durch Hülfssatz 15 angewiesene Zahl $\varkappa$ durch p teilbar, so bilden wir die Zahl $\varrho = \varkappa^{s'-1}$. Da nach Hülfssatz 15 andererseits $\varkappa^{s'+1} = \alpha^4$ sein soll, wo α in $k(i)$ liegt, so folgt $\varkappa^2 = \varrho^{-1}\alpha^4$, d. h. $\sqrt{\varkappa} = \alpha\sqrt[4]{\varrho^{-1}}$. In Folge dessen ist ϱ das Quadrat einer Zahl in $k(i)$; wir können $\varrho = \frac{\tau^2}{a^4}$ setzen in solcher Weise, dass τ eine ganze, zu p prime Zahl in $k(i)$ und a eine ganze rationale Zahl bedeutet. Da der Körper $k(i, C_1)$ mit dem Körper $k(i, \sqrt{\tau})$ übereinstimmt, und da anderer-

seits die Relativdiscriminante der Zahl $\sqrt{\tau}$ in Bezug auf $k(i)$ zu p prim ist, so ist auch die Relativdiscriminante des Körpers $k(i, C_1)$ in Bezug auf $k(i)$ prim zu p, und hieraus folgt, dass die Discriminante von C_1 nicht durch p teilbar ist, entgegen der Voraussetzung.

Ist im Falle $l=2$ der Exponent $h>2$, so setzen wir $Z=e^{\frac{i\pi}{2^{h-1}}}$. Nehmen wir dann an, es gäbe eine in der Discriminante von C_1 aufgehende Primzahl $p\equiv 1$ nach 4 und $\not\equiv 1$ nach 2^h, und ist $\mathfrak{p}$ ein idealer Primfactor von p in $k(Z)$, so bliebe $\mathfrak{p}$ ungeändert bei einer Substitution $s_*^{2^{h-3}}$, wo s_* entweder $=(Z:Z^5)$ oder $=(Z:Z^{-5})$ zu nehmen ist; folglich wäre $\mathfrak{p}^{s_*^{2^{h-3}}-1}=1$. Wegen $(\pm 5)^{2^{h-3}}\not\equiv 1$ nach 2^h würde, ähnlich wie oben, eine Gleichung von der Gestalt:

$$2^{h-1}=(s_*^{2^{h-3}}-1)\varphi(s_*)+(s_*\mp 5)\psi(s_*)+2^h\chi(s_*)$$

gelten, und aus dieser schliessen wir, wie vorhin bei ungeradem l, auf einen Widerspruch mit der Annahme, wonach p in der Discriminante von C_1 aufgeht. Damit ist der Hülfssatz 16 vollständig bewiesen.

Aus dem Hülfssatze 16 folgt ohne Schwierigkeit die weitere Thatsache:

Hülfssatz 17. Es sei C_h ein cyklischer Körper von einem Grade l^h, wo l eine beliebige Primzahl ($=2$ oder $\neq 2$) ist; der Unterkörper $l$ten Grades von C_h werde mit C_1 bezeichnet; die Discriminante des Körpers C_1 enthalte die von l verschiedene Primzahl p: dann kann stets ein Abel'scher Körper $C'_{h'}$ von einem gewissen Grade $l^{h'}\leqq l^h$ mit folgenden beiden Eigenschaften gefunden werden:

Erstens. Der aus $C'_{h'}$ und einem gewissen Kreiskörper P_h zusammengesetzte Körper enthält C_h als Unterkörper.

Zweitens. Die Discriminante des Körpers $C'_{h'}$ enthält nur solche Primzahlen, die auch in der Discriminante des Körpers C aufgehen, darunter aber nicht die Primzahl p.

Beweis. Nach Hülfssatz 16 besitzt die rationale Primzahl p die Congruenzeigenschaft $p\equiv 1$ nach l^h; man construire nach § 100 den cyklischen Kreiskörper P_h vom Grade l^h, dessen Discriminante eine Potenz von p ist, und betrachte den aus C und P_h zusammengesetzten Körper $k(C_h, P_h)$, dessen Grad $l^{h+h'}$ sei. In P_h gilt $p=\mathfrak{p}^{l^h}$, wo $\mathfrak{p}$ ein Primideal in P_h bedeutet. Es sei $\mathfrak{P}$ ein in $\mathfrak{p}$ aufgehendes Primideal des Körpers $k(C_h, P_h)$. Da das Primideal $\mathfrak{P}$ in der Gradzahl $l^{h+h'}$ des Körpers $k(C_h, P_h)$ nicht aufgeht, so ist dieser Körper $k(C_h, P_h)$ Verzweigungskörper des Primideals $\mathfrak{P}$ und als solcher nach Satz 81 relativ

cyklisch, und zwar mindestens vom Relativgrade l^h, in Bezug auf den Trägheitskörper des Primideals $\mathfrak{P}$, der $C'_{h'}$ heisse. Da ferner cyklische Körper von höherem als dem l^hten Grade in $k(C_h, P_h)$ nicht vorkommen können, so hat $k(C_h, P_h)$ genau den Relativgrad l^h in Bezug auf $C'_{h'}$. Hieraus folgt, dass der Körper $C'_{h'}$ vom Grade $l^{h'}$ ist. Die Differente des Trägheitskörpers $C'_{h'}$ ist nach Satz 76 nicht durch $\mathfrak{P}$ teilbar, und daher ist, mit Rücksicht auf Satz 68, die Discriminante des Körpers $C'_{h'}$ nicht durch p teilbar. Andererseits enthält diese Discriminante wegen Satz 39 nur solche rationale Primzahlen, welche in der Discriminante von C_h aufgehen. Endlich folgt aus Satz 87, dass der aus $C'_{h'}$ und P_h zusammengesetzte Körper mit $k(C_h, P_h)$ übereinstimmt. Der Körper $C'_{h'}$ besitzt demnach alle im Hülfssatz 17 verlangten Eigenschaften.

§ 103.

Der cyklische Körper vom Grade u, dessen Discriminante nur u enthält, und die cyklischen Körper vom Grade u^h und 2^h, in denen U_1 bez. H_1 als Unterkörper enthalten ist.

Hülfssatz 18. Wenn die Discriminante eines cyklischen Körpers C_1 von einem ungeraden Primzahlgrade u ausschliesslich die Primzahl u enthält, so stimmt C_1 mit U_1 überein.

Beweis. Wir setzen $\zeta = e^{\frac{2i\pi}{u}}$ und $s = (\zeta : \zeta^r)$, wo r eine Primitivzahl nach u bedeute. Schreiben wir überdies $\lambda = 1 - \zeta$, so ist $\mathfrak{l} = (\lambda)$ ein Primideal in $k(\zeta)$, und es wird im Sinne der Idealtheorie $u = \mathfrak{l}^{u-1}$; endlich gilt die Congruenz

$$s\lambda = 1 - \zeta^r \equiv r\lambda, \quad (\mathfrak{l}^2).$$

Wir betrachten nun die uns durch Hülfssatz 15 angewiesene Zahl $\varkappa$. Da das Primideal $\mathfrak{l}$ in $k(\zeta)$ vom ersten Grade ist, so folgt, wenn $\varrho = \varkappa^{(s-1)(u-1)}$ gesetzt wird, in Anbetracht der Gleichung $s\mathfrak{l} = \mathfrak{l}$ und nach Satz 24 die Congruenz $\varrho \equiv 1$ nach $\mathfrak{l}$. Da $r - 1$ zu u prim ist, so wird der aus C_1 und $k(\zeta)$ zusammengesetzte Körper auch durch ζ und $\sqrt[u]{\varrho}$ bestimmt sein. Wir setzen $\varrho \equiv 1 + a\lambda$ nach $\mathfrak{l}^2$, wo a eine ganze rationale Zahl bedeute; dann ist $\sigma = \varrho\zeta^a \equiv 1$ nach $\mathfrak{l}^2$.

Nunmehr führen wir den Nachweis dafür, dass die Congruenz $\sigma \equiv 1$ nach $\mathfrak{l}^u$ besteht. Zu dem Zwecke nehmen wir an, es sei $\sigma \equiv 1 + a\lambda^e$

nach $\mathfrak{l}^{e+1}$, wobei der Exponent $e < u$ ausfällt und a eine nicht durch u teilbare ganze rationale Zahl bedeutet.

Wir berücksichtigen, dass nach dem Hülfssatze 15 $\varkappa^{s-r}$ und folglich auch σ^{s-r} die $u$te Potenz einer Zahl in $k(\zeta)$ ist; wir setzen $\sigma^{s-r} = \beta^u$, wo β eine Zahl des Körpers $k(\zeta)$ sei. Diese Gleichung liefert die Congruenz $1 + a(r\lambda)^e - ar\lambda^e \equiv \beta^u$ nach $\mathfrak{l}^{e+1}$. Aus dieser folgt zunächst $\beta \equiv 1$ nach $\mathfrak{l}$, und dies liefert $\beta^u \equiv 1$ nach $\mathfrak{l}^u$. Hieraus würde endlich $ar^e \equiv ar$ nach $\mathfrak{l}$ folgen, was unmöglich ist, da r Primitivzahl nach u sein soll und $e > 1$ ist. Diese Betrachtung lehrt die Richtigkeit der Congruenz $\sigma \equiv 1$ nach $\mathfrak{l}^u$.

Wir setzen nun $\sigma = \dfrac{\tau}{a^{u(u-1)}}$ in solcher Weise, dass τ eine ganze Zahl in $k(\zeta)$ und a eine ganze rationale Zahl bedeutet; es ist dann $\tau \equiv 1$ nach $\mathfrak{l}^u$ Nehmen wir nun an, der Körper C_1 sei von dem Körper U_1 verschieden, so entsteht durch Zusammensetzung aus $k(\zeta)$, U_1 und C_1 der durch $\sqrt[u]{\zeta}$ und $\sqrt[u]{\tau}$ bestimmte Körper $k(\sqrt[u]{\zeta}, \sqrt[u]{\tau})$ vom Grade $u^2(u-1)$. Es ist andererseits $\xi = \dfrac{1-\sqrt[u]{\tau}}{\lambda}$, wie die Gleichung $\dfrac{(\xi\lambda-1)^u+\tau}{\lambda^u} = 0$ zeigt, eine ganze Zahl des Körpers $k(\sqrt[u]{\zeta}, \sqrt[u]{\tau})$, und die Relativdiscriminante dieser Zahl in Bezug auf $k(\sqrt[u]{\zeta})$ ist gleich $\varepsilon\tau^{u-1}$, wo ε eine Einheit ist. Da τ zu u prim ist, so ist mithin die Relativdiscriminante des Körpers $k(\sqrt[u]{\zeta}, \sqrt[u]{\tau})$ in Bezug auf den Körper $k(\sqrt[u]{\zeta})$ ebenfalls prim zu u. Bezeichnen wir daher mit $\mathfrak{L}^*$ einen idealen Primfactor von $\mathfrak{l}$ im Körper $k(\sqrt[u]{\zeta}, \sqrt[u]{\tau})$, so besitzt $\mathfrak{L}^*$ mit Rücksicht auf Satz 93 in diesem Körper einen Trägheitskörper T, welcher den Grad u hat. Die Discriminante dieses Trägheitskörpers T ist prim zu u, und wegen Satz 85 müsste sie daher den Wert $+1$ oder -1 besitzen. Dass es aber einen cyklischen Körper vom Primzahlgrade u mit der Discriminante ± 1 nicht giebt, folgt entweder direct aus Satz 44 oder mittelst Satz 94, wenn wir den in diesem Satze 94 mit k bezeichneten Körper gleich dem Körper der rationalen Zahlen nehmen und die Thatsache berücksichtigen, dass im Körper der rationalen Zahlen alle Ideale Hauptideale sind. Damit ist der Beweis für den Hülfssatz 18 erbracht.

Hülfssatz 19. Wenn ein cyklischer Körper C_h vom Grade l^h, wo

l gleich einer ungeraden Primzahl u oder gleich 2 ist, den Körper U_1 bez. II_1 als Unterkörper enthält, so ist C_h Unterkörper eines solchen Körpers, welcher aus U_h bez. II_h und aus einem gewissen cyklischen Körper $C'_{h'}$ von einem Grade $l^{h'} < l^h$ durch Zusammensetzung entsteht.

Beweis. Es sei $C_h \neq U_h$ bez. II_h. Der grösste sowohl in C_h als in U_h bez. II_h enthaltene Unterkörper werde mit L_{h^*} bezeichnet; L_{h^*} habe den Grad l^{h^*}, wo h^* eine positive ganze rationale Zahl $< h$ bedeute. Es sei t eine solche Substitution aus der Gruppe des Körpers C_h, welche mit ihren Potenzen diese Gruppe erzeugt, und z eine solche Substitution, welche die Gruppe des Körpers U_h bez. II_h erzeugt. Setzen wir $t^* = t^{l^{h^*}}$ und $z^* = z^{l^{h^*}}$, so erzeugen t^* und z^* beide Male diejenigen Untergruppen vom Grade l^{h-h^*}, zu denen L_{h^*} als Unterkörper einerseits von C_h, andererseits von U_h bez. II_h gehört. Der aus C_h und U_h bez. II_h zusammengesetzte Körper K ist in Bezug auf L_{h^*} vom Relativgrade l^{2h-2h^*} und daher überhaupt vom Grade l^{2h-h^*}.

Um die Gruppe G des Körpers K zu ermitteln, bezeichnen wir mit ϑ eine den Körper C_h und mit γ eine den Körper U_h bez. II_h bestimmende Zahl und verstehen unter x, y unbestimmte Parameter. Die Grösse $\Theta = x\vartheta + y\gamma$ genügt einer Gleichung vom l^{2h-h^*}ten Grade, deren Coefficienten ganzzahlige Functionen von x und y sind, und welche in dem durch die Parameter x und y bestimmten Rationalitätsbereich irreducibel ist. Die verschiedenen Wurzeln dieser Gleichung sind von der Gestalt

$$\Theta_{mn} = xt^m\vartheta + yz^n\gamma,$$

wo m, n gewisse Paare ganzer Zahlen bedeuten. Da einem bekannten Satze zufolge sowohl ϑ wie γ sich als rationale Functionen von Θ ausdrücken lassen, wobei die Coefficienten ganzzahlige Functionen von x und y werden, so sind auch die Grössen Θ_{mn} ebenso ausdrückbar; wir setzen

$$\Theta_{mn} = xt^m\vartheta + yz^n\gamma = \Phi_{mn}(\Theta),$$

wobei Φ_{mn} eine rationale Function von Θ bedeutet, deren Coefficienten ganzzahlige Functionen von x, y sind. Es bezeichne nun A irgend eine Zahl in K oder überhaupt eine rationale Function von x, y, deren Coefficienten in K liegen; dann wird A gleich einer rationalen Function $F(\Theta)$ der Grösse Θ, deren Coefficienten ganzzahlige Functionen von x, y sind. Es drücken sich ferner die zu A conjugirten Grössen in der Gestalt

$$S_{mn}A = F(\Phi_{mn}(\Theta))$$

aus, und das System der betreffenden l^{2h-h^*} Substitutionen S_{mn} bildet die Gruppe G des Körpers K. Wegen

$$S_{mn}\Theta = xS_{mn}\vartheta + yS_{mn}\gamma = xt^m\vartheta + yz^n\gamma$$

wird

$$S_{mn}\vartheta = t^m\vartheta, \quad S_{mn}\gamma = z^n\gamma,$$

und hieraus folgt leicht:

$$(41.) \qquad S_{mn}S_{m'n'} = S_{m+m',\, n+n'},$$

wenn allgemein die Festsetzung $S_{mn} = S_{m^*n^*}$ getroffen wird, falls $m \equiv m^*$ und $n \equiv n^*$ nach l^h ist. Aus (41.) folgt die Vertauschung der Substitution der Gruppe G, d. h. der Körper K ist ein Abel'scher Körper.

Es bezeichne r eine Primitivzahl nach l^h; da insbesondere $z^r\gamma$ eine zu γ conjugirte Zahl ist, so muss es jedenfalls eine Substitution in der Gruppe G geben, bei welcher der zweite Index $n \equiv r$ nach l^h ist. Wir setzen eine solche Substitution $S_{mr} = s$. Der Grad der aus s erzeugten cyklischen Gruppe ist l^h. Es kann ferner leicht erkannt werden, dass alle diejenigen Substitutionen der Gruppe G, bei denen der zweite Index $\equiv 0$ nach l^h ausfällt, für sich eine cyklische Untergruppe vom Grade l^{h-h^*} bilden. Es sei $s^* = S_{m^*0}$ eine erzeugende Substitution dieser cyklischen Gruppe. Die Gruppe G entsteht dann offenbar durch Zusammensetzung aus den l^h Potenzen von s und den l^{h-h^*} Potenzen von s^*. Zu der aus den Potenzen von s^* bestehenden Untergruppe gehört offenbar im Körper K der cyklische Unterkörper U_h bez. II_h. Zu der aus s erzeugten Gruppe gehört in K ein gewisser cyklischer Unterkörper $C'_{h'}$ vom Grade l^{h-h^*}. Die beiden Körper U_h bez. II_h und $C'_{h'}$ haben keinen gemeinsamen Unterkörper ausser dem Körper der rationalen Zahlen, und der Körper K entsteht daher durch Zusammensetzung aus diesen beiden cyklischen Körpern. Damit ist der Hülfssatz 19 vollständig bewiesen.

§ 104.

Beweis des Fundamentalsatzes über Abel'sche Körper.

Wir beweisen nunmehr den Fundamentalsatz 131 in folgender Art. Zunächst ist in § 48 festgestellt worden, dass jeder Abel'sche Körper sich aus cyklischen Körpern zusammensetzen lässt, deren Grade Primzahlen oder Primzahlpotenzen sind; es ist daher nur nötig, zu zeigen, dass jeder cyklische Körper C_h von einem Grade l^h, wo l eine Primzahl bezeichnet, ein Kreiskörper ist.

Um diesen Beweis zu führen, nehmen wir an, es sei bereits die Richtigkeit des Fundamentalsatzes 131 für alle diejenigen Abel'schen Körper erkannt, deren Grad eine niedere Potenz von l als l^h ist.

Es werde nun der in C_h enthaltene Unterkörper vom l ten Grade C_1 in's Auge fasst. Nehmen wir an, dass die Discriminante von C_1 eine von l verschiedene rationale Primzahl p enthält, so ist nach Satz 39 auch die Discriminante von C_h durch p teilbar. Ferner existirt nach Hülfssatz 17 ein Abel'scher Körper $C'_{h'}$ vom Grade $l^{h'} \leqq l^h$ der Art, dass C_h Unterkörper des aus $C'_{h'}$ und dem Kreiskörper P_h zusammengesetzten Körpers wird. Ist dann $C'_{h'}$ ein cyklischer Körper von niederem als l^h ten Grade oder aus mehreren solchen cyklischen Körpern zusammengesetzt, so erweist sich $C'_{h'}$ auf Grund unserer Annahme als Kreiskörper, und mithin ist auch C_h ein Kreiskörper. Es ist demnach nur noch der Fall in Betracht zu ziehen, dass $h' = h$ ausfällt und $C'_{h'} = C'_h$ ein cyklischer Körper vom Grade l^h ist. Wie der vorhin angewandte Hülfssatz 17 aussagt, enthält die Discriminante von C'_h nur solche Primzahlen, welche in der Discriminante von C_h aufgehen, aber nicht die Primzahl p; die Discriminante von C'_h enthält also mindestens eine rationale Primzahl weniger als die Discriminante von C_h.

Wir bezeichnen den Unterkörper l ten Grades von C'_h mit C'_1. Geht dann in der Discriminante von C'_1 noch eine von l verschiedene rationale Primzahl p' auf, so können wir auf den Körper C'_h dass nämliche Verfahren anwenden, das wir soeben für den ursprünglich vorgelegten Körper C_h dargelegt haben, und gelangen dann entweder zu der Einsicht, dass C'_h ein Kreiskörper ist, oder wir werden auf einen cyklischen Körper C''_h vom Grade l^h geführt, dessen Discriminante wieder mindestens eine rationale Primzahl, nämlich die Primzahl p', weniger enthält als die Discriminante des Körpers C'_h. Das so eingeleitete Verfahren führt nach einer gewissen Anzahl m sich folgender Anwendungen entweder auf einen Körper $C^{(m)}_{h^{(m)}}$, der sich auf Grund unserer Annahme bereits als Kreiskörper erweist, oder wir gelangen schliesslich zu einem cyklischen Körper $C^{(m)}_h$ vom Grade l^h von der Art, dass der in $C^{(m)}_h$ enthaltene Unterkörper $C^{(m)}_1$ vom l ten Grade eine Discriminante besitzt, welche keine rationale Primzahl oder nur die Primzahl l enthält. Da es nach den Bemerkungen auf S. 347 einen cyklischen Körper l ten Grades mit der Discriminante ± 1 nicht giebt, so tritt notwendig der letztere Umstand ein.

Wir unterscheiden nunmehr zwei Fälle, je nachdem l eine ungerade Primzahl u oder gleich 2 ist.

Im ersteren Falle stimmt nach Hülfssatz 18 $C_1^{(m)}$ mit U_1 überein.

Im zweiten Falle $l=2$ ist, wenn $h=1$ ausfällt, der Körper $C_h^{(m)}=C_1^{(m)}$ entweder gleich $k(i)$ oder gleich $k(\sqrt{2})=II_1$ und mithin offenbar ein Kreiskörper. Für $h>1$ erweist sich jedoch $C_1^{(m)}$ stets gleich $k(\sqrt{2})=II_1$. Ist nämlich $C_h^{(m)}$ ein reeller Körper, so ist offenbar auch $C_1^{(m)}$ reell, und daraus folgt die Behauptung. Ist jedoch $C_h^{(m)}$ ein imaginärer Körper, so bilden die sämtlichen reellen Zahlen desselben einen reellen Unterkörper von Grade 2^{h-1}, und da $C_1^{(m)}$ notwendig in diesem reellen Körper enthalten ist, so ist $C_1^{(m)}$ ebenfalls reell und stimmt also mit II_1 überein.

In den beiden oben unterschiedenen Fällen ist somit, wenn wir von $l=2$, $h=1$ absehen, stets der Körper $C_1^{(m)}=U_1$ bez. $=II_1$. Nach Hülfssatz 19 ist infolgedessen $C_h^{(m)}$ Unterkörper eines Körpers, der sich aus U_h bez. II_h und einem cyklischen Körper $C_{\bar{h}}$ vom Grade $l^{\bar{h}}<l^h$ zusammensetzt. Da nun der Fundamentalsatz 131 für cyklische Körper von der letzteren Beschaffenheit bereits als bewiesen angenommen worden ist, so erweist sich auch $C_h^{(m)}$ als Kreiskörper. Damit ist der Fundamentalsatz 131 vollständig bewiesen, und zugleich ist ersichtlich, in welcher Weise man alle Abel'schen Körper von gegebener Gruppe und gegebener Discriminante aufstellen kann.

Capitel XXIV.

Die Wurzelzahlen des Kreiskörpers der $l$ten Einheitswurzeln.

§ 105.

Die Definition und Existenz der Normalbasis.

Eine Basis eines Abel'schen Körpers K von einem Grade M soll eine **Normalbasis** heissen, wenn sie aus einer ganzen Zahl N des Körpers K und den zu N conjugirten Zahlen $N', \ldots, N^{(M-1)}$ besteht. Es gilt der folgende Hülfssatz:

Hülfssatz 20. Wenn ein Abel'scher Körper K eine Normalbasis besitzt, so besitzt auch jeder Unterkörper k des Körpers K eine Normalbasis.

Beweis. Es sei M der Grad von K, und es seien $t_1, \ldots, t_M$ die Substitutionen der Gruppe des Abel'schen Körpers K; ferner sei N eine solche ganze Zahl in K, die mit ihren conjugirten zusammen eine Normalbasis von K liefert. Bilden dann $t_1, \ldots, t_r$ diejenige Untergruppe jener Gruppe von M Substitutionen, zu welcher der Unterkörper k von K gehört, so kann man dazu unter jenen M Substitutionen $t_1, \ldots, t_M$ solche $m = \frac{M}{r}$ Substitutionen $t'_1, \ldots, t'_m$ finden, dass die M Substitutionen $t_1, \ldots, t_M$, abgesehen von ihrer Reihenfolge, durch die Substitutionenproducte

$$t'_1 t_1, \ldots, t'_1 t_r; \quad t'_2 t_1, \ldots, t'_2 t_r; \quad \ldots; \quad t'_m t_1, \ldots, t'_m t_r$$

dargestellt werden. Ist α eine ganze Zahl in k, so gilt, da eine solche stets auch eine ganze Zahl in K ist, eine Gleichung

$$\alpha = a_{11} t'_1 t_1 N + \cdots + a_{1r} t'_1 t_r N + \cdots + a_{m1} t'_m t_1 N + \cdots + a_{mr} t'_m t_r N,$$

wo $a_{11}, \ldots, a_{1r}, \ldots, a_{m1}, \ldots, a_{mr}$ ganze rationale Zahlen sind. Berücksichtigen wir, dass α bei Anwendung der einzelnen Substitutionen $t_1, \ldots, t_r$ ungeändert bleibt, und andererseits, dass zwischen den $M = mr$ Zahlen $t'_1 t_1 N, \ldots, t'_1 t_r N; \ldots; t'_m t_1 N, \ldots, t'_m t_r N$ keine lineare Relation mit ganzzahligen, nicht sämtlich verschwindenden Coefficienten stattfinden kann, so folgt offenbar:

$$a_{11} = a_{12} = \cdots = a_{1r}, \quad \ldots, \quad a_{m1} = a_{m2} = \cdots = a_{mr},$$

d. h.: wenn

$$\nu = t_1 N + t_2 N + \cdots + t_r N$$

gesetzt wird, so bilden die m Zahlen $t'_1 \nu, t'_2 \nu, \ldots, t'_m \nu$ eine Normalbasis des Körpers k.

Satz 132. Ein jeder Abel'sche Körper K vom Mten Grade, dessen Discriminante D zu M prim ist, besitzt eine Normalbasis.

Beweis. Die verschiedenen rationalen Primzahlen in D seien $p, p', \ldots$. Da keine dieser Primzahlen in M aufgeht, so ist nach dem Beweise des Satzes 131 der Abel'sche Körper K in demjenigen Kreiskörper als Unterkörper enthalten, welcher durch die Zahlen $\zeta = e^{\frac{2i\pi}{p}}, \zeta' = e^{\frac{2i\pi}{p'}}, \ldots$, d. h. welcher durch die Einheitswurzel $Z = e^{\frac{2i\pi}{pp'\cdots}}$ bestimmt ist. Für den Körper $k(\zeta)$ bilden nach Satz 118 die Zahlen $1, \zeta, \ldots, \zeta^{p-2}$ und folglich

auch die Zahlen $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ eine Basis; die letztere Basis ist eine Normalbasis. Entsprechendes gilt für $k(\zeta'), \ldots$.

Man bilde nun das System der $(p-1)(p'-1)\ldots$ Zahlen $\zeta^h \zeta'^{h'}\ldots$, wo die Exponenten h; h'; ... bez. die Zahlen

$$1, \; 2, \; \ldots, \; p-1; \; 1, \; 2, \; \ldots, \; p'-1; \; \ldots$$

unabhängig von einander durchlaufen sollen; dann stellt dieses System von $\Phi(pp'\ldots)$ Zahlen nach Satz 88 eine Basis des Körpers $k(Z)$ dar, und diese Basis ist offenbar eine Normalbasis. Nach dem Hülfssatz 20 besitzt folglich auch der Abel'sche Körper K eine Normalbasis. Damit ist der Satz 132 bewiesen.

§ 106.

Der Abel'sche Körper vom Primzahlgrade l und von der Discriminante p^{l-1}. Die Wurzelzahlen dieses Körpers.

Die einfachsten und wichtigsten Abel'schen Körper nächst den quadratischen Körpern sind diejenigen, bei welchen der Grad eine ungerade Primzahl l ist und die Discriminante d nur eine einzige, und zwar von l verschiedene Primzahl p enthält. Es bedeute k einen solchen Körper. Nach Hülfssatz 16 besitzt die Primzahl p notwendig die Congruenzeigenschaft $p \equiv 1$ nach l. Die Primzahl p wird im Körper k die $l$te Potenz eines Primideales ersten Grades. Nach den Bemerkungen zu Satz 79 und mit Rücksicht darauf, dass k jedenfalls ein reeller Körper, also d positiv ist, ergiebt sich $d = p^{l-1}$.

Es seien $1, t, t^2, \ldots, t^{l-1}$ die Substitutionen der Gruppe des Körpers k, und die Zahlen $\nu, t\nu, \ldots, t^{l-1}\nu$ mögen eine Normalbasis von k bilden (s. Satz 132). Die Zahl ν ist dann jedenfalls eine den Körper k bestimmende Zahl. Es werde $\zeta = e^{\frac{2i\pi}{l}}$ gesetzt; der Ausdruck

$$\Omega = \nu + \zeta . t\nu + \zeta^2 . t^2\nu + \cdots + \zeta^{l-1} . t^{l-1}\nu$$

soll eine **Wurzelzahl** des Körpers $k = k(\nu)$ heissen.

Jede solche Wurzelzahl Ω ist offenbar eine ganze Zahl des aus $k(\nu)$ und $k(\zeta)$ zusammengesetzten Körpers $k(\nu, \zeta)$. Das Studium der vorhandenen Normalbasen und Wurzelzahlen des Abel'schen Körpers $k(\nu)$ giebt uns wichtige Aufschlüsse über die in p aufgehenden Primideale des Körpers $k(\zeta)$. Die Ausführungen dieses Capitels erfahren nur leichte Abänderungen, wenn statt der ungeraden Primzahl l die Zahl 2 genommen wird.

§ 107.
Die charakteristischen Eigenschaften der Wurzelzahlen.

Satz 133. Es sei ein Abel'scher Körper k vom Grade l und mit der Discriminante $d=p^{l-1}$ vorgelegt, wo l und p verschiedene ungerade Primzahlen bedeuten; ferner sei $\nu, t\nu, \ldots, t^{l-1}\nu$ eine Normalbasis dieses Körpers k. Wird dann $\zeta=e^{\frac{2i\pi}{l}}$, $\mathfrak{l}=(1-\zeta)$ und $s=(\zeta:\zeta^r)$ gesetzt, wo r eine Primitivzahl nach l bedeute, so besitzt die aus jener Normalbasis entspringende Wurzelzahl Ω des Körpers $k=k(\nu)$ die folgenden drei Eigenschaften:

Erstens. Die $l$te Potenz der Wurzelzahl, $\omega=\Omega^l$, ist eine Zahl des Kreiskörpers $k(\zeta)$, und zudem wird ω^{s-r} gleich der $l$ten Potenz einer Zahl des Körpers $k(\zeta)$.

Zweitens. Es gelten die sich gegenseitig bedingenden Congruenzen

$$\Omega\equiv\pm1,\quad(\mathfrak{l}),\qquad \omega\equiv\pm1,\quad(\mathfrak{l}^l).$$

Drittens. $n(\omega)$, die Norm der Zahl ω in $k(\zeta)$, ist $=p^{\frac{l(l-1)}{2}}$.

Beweis. Die Zahlen Ω^l und Ω^{s-r} sind solche Zahlen in $k(\zeta,\nu)$, welche beim Uebergang von ν in $t\nu$ ungeändert bleiben. Sie sind deshalb Zahlen in $k(\zeta)$. Hieraus folgt die erste in Satz 133 angegebene Eigenschaft.

Da $\nu, t\nu, \ldots, t^{l-1}\nu$ Basiszahlen des Körpers $k(\nu)$ sind, so gilt insbesondere

$$1 = a_0\nu+a_1t\nu+\cdots+a_{l-1}t^{l-1}\nu$$

für bestimmte ganze rationale Zahlen $a_0, a_1, \ldots, a_{l-1}$. Die Anwendung der Substitution t auf diese Formel lehrt, dass $a_0=a_1=\cdots=a_{l-1}$ ist, und da die Coefficienten $a_0, a_1, \ldots, a_{l-1}$ keinen gemeinsamen Teiler $\neq\pm1$ haben können, so haben sie sämtlich den gleichen Wert ±1, d. h. es ist $\nu+t\nu+\cdots+t^{l-1}\nu=\pm1$. Aus dieser Formel folgt:

$$\Omega=\nu+\zeta.t\nu+\zeta^2.t^2\nu+\cdots+\zeta^{l-1}.t^{l-1}\nu$$
$$\equiv\nu+t\nu+\cdots+t^{l-1}\nu\equiv\pm1,\quad(\mathfrak{l}).$$

Mit Hülfe von $\omega\mp1=(\Omega\mp1)(\zeta\Omega\mp1)\ldots(\zeta^{l-1}\Omega\mp1)$ erkennen wir die zweite Eigenschaft der Zahl ω.

Endlich folgt durch eine geeignete Anwendung des Multiplications-

satzes der Determinanten

$$\begin{vmatrix} \nu, & t\nu, & \ldots, & t^{l-1}\nu \\ t^{l-1}\nu, & \nu, & \ldots, & t^{l-2}\nu \\ \cdot & \cdot & \cdot & \cdot \\ t\nu, & t^2\nu, & \ldots, & \nu \end{vmatrix} = (\nu + t\nu + \cdots + t^{l-1}\nu)\, n(\Omega) = \pm n(\Omega),$$

wo

$$n(\Omega) = (\nu + \zeta t\nu + \cdots + \zeta^{l-1} t^{l-1}\nu) \ldots (\nu + \zeta^{l-1} t\nu + \cdots + \zeta^{(l-1)^2} t^{l-1}\nu)$$

die Relativnorm von Ω in Bezug auf den Körper $k(\nu)$ ist. Das Quadrat der Determinante linker Hand ist gleich der Discriminante des Körpers $k(\nu)$, d. h. $= p^{l-1}$, und folglich ergiebt sich

$$n(\omega) = (n(\Omega))^l = p^{l\left(\frac{l-1}{2}\right)}.$$

Damit ist der Satz 133 vollständig bewiesen.

Die drei in Satz 133 bewiesenen Eigenschaften einer Wurzelzahl Ω des Körpers $k(\nu)$ reichen umgekehrt völlig zur Charakterisirung einer solchen Zahl hin. Es gilt nämlich folgende Thatsache:

Satz 134. Es sei l eine ungerade Primzahl und $\zeta = e^{\frac{2i\pi}{l}}$, ferner p eine Primzahl $\equiv 1$ nach l; wenn dann ω eine solche Zahl des Kreiskörpers $k(\zeta)$ bedeutet, die nicht gleich der $l$ten Potenz einer Zahl in $k(\zeta)$ wird, und welche die drei in Satz 133 angegebenen Eigenschaften besitzt, so ist $\Omega = \sqrt[l]{\omega}$ eine Wurzelzahl des Abel'schen Körpers $l$ten Grades von der Discriminante p^{l-1}.

Beweis. Die Zahl $\Omega = \sqrt[l]{\omega}$ bestimmt einen relativ Galois'schen Körper vom Relativgrade l in Bezug auf den Körper $k(\zeta)$. Es sei t diejenige Substitution der Relativgruppe, für welche $t\Omega = \zeta^{-1}\Omega$ wird. Mit Rücksicht auf die erste Eigenschaft der Zahl ω, die sich in der Formel $s\omega = \omega_r \alpha^l$ ausdrückt, wo α eine Zahl in $k(\zeta)$ bedeutet, ist der durch ζ und Ω bestimmte Körper vom $l(l-1)$ten Grade ein Galois'scher Körper. Die Zahl α erfüllt die Bedingung

$$\omega^{1-r^{l-1}} = \alpha^{l\frac{s^{l-1}-r^{l-1}}{s-r}};$$

wir legen sie eindeutig fest durch die weitere Forderung

$$\omega^{\frac{1-r^{l-1}}{l}} = \alpha^{\frac{s^{l-1}-r^{l-1}}{s-r}}.$$

Wir wollen nun unter t und s zugleich diejenigen bestimmten Substitutionen der Gruppe dieses Galois'schen Körpers $k(\zeta, \Omega)$ verstehen, welche neben den für t und s schon festgesetzten Beziehungen noch $t\zeta = \zeta$ und $s\Omega = \Omega^r\alpha$ ergeben. Diese beiden Substitutionen s und t sind mit einander vertauschbar, da

$$st\Omega = \zeta^{-r}\Omega^r\alpha = ts\Omega$$

wird, d. h. der Körper $k(\zeta, \Omega)$ ist ein Abel'scher Körper. Ferner wird die Untergruppe der Gruppe von $k(\zeta, \Omega)$, welche aus den Potenzen der Substitution s besteht, genau vom Grade $l-1$. Der zu dieser Untergruppe gehörige Unterkörper von $k(\zeta, \Omega)$ ist daher vom $l$ten Grade; er ist wiederum ein Abel'scher Körper; dieser Körper werde mit k bezeichnet.

Wir beweisen zunächst, dass die Discriminante dieses Körpers k zu l prim ist. Da $\Omega \equiv \pm 1$ nach $\mathfrak{l} = (1-\zeta)$ ist, so stellt der Quotient $\dfrac{\Omega \mp 1}{1-\zeta}$ eine ganze Zahl dar. Wegen $t\Omega = \zeta^{-1}\Omega$ hat die Relativdifferente dieser ganzen Zahl in Bezug auf den Körper $k(\zeta)$ den Wert $\varepsilon\Omega^{l-1}$, wo ε eine Einheit bedeutet, und daher ist die Relativdifferente des Körpers $k(\zeta, \Omega)$ in Bezug auf den Körper $k(\zeta)$ prim zu l. Bedeutet $\mathfrak{L}$ ein in $\mathfrak{l}$ aufgehendes Primideal des Körpers $k(\zeta, \Omega)$, so kommt dieses nach Satz 93 in $\mathfrak{l}$ zu keiner höheren als der ersten Potenz vor, d. h. es ist $l = \mathfrak{L}^{l-1}\mathfrak{M}$, wo $\mathfrak{M}$ sich nicht mehr durch $\mathfrak{L}$ teilen lässt. Hieraus folgt nach § 39 und § 40, dass der Trägheitskörper des Primideals $\mathfrak{L}$ vom Grade l sein muss, und daher ist k selbst dieser Trägheitskörper. Nach Satz 76 ist die Differente des Körpers k nicht durch $\mathfrak{L}$ und folglich auf Grund des Satzes 68 auch die Discriminante des Körpers k nicht durch l teilbar.

Wir setzen

$$(41.) \qquad \nu = \frac{\pm 1 + \Omega + s\Omega + s^2\Omega + \cdots + s^{l-2}\Omega}{l},$$

wo das Vorzeichen das nämliche wie in den Congruenzen $\Omega \equiv \pm 1$, $s\Omega \equiv \pm 1, \ldots$ nach $\mathfrak{l}$ ist; dann wird der Zähler dieses in gebrochener Form erscheinenden Ausdrucks (41.) congruent 0 nach $\mathfrak{l}$. Dieser Zähler stellt eine Zahl in k dar. Ist l in k Primideal, so muss daher dieser Zähler auch durch l teilbar sein, und es ist ν eine ganze Zahl. Anderenfalls haben wir im Körper k, da die Discriminante von k nicht den Factor l enthält, eine Zerlegung $l = \mathfrak{l}_1 \ldots \mathfrak{l}_l$, wo $\mathfrak{l}_1, \ldots, \mathfrak{l}_l$ von einander verschiedene Primideale sind, und im Körper $k(\zeta, \Omega)$ gilt dann, wie man mit

Hülfe von Satz 88 erkennt, die Zerlegung

$$\mathfrak{l} = (1-\zeta) = (\mathfrak{l},\ \mathfrak{l}_1)(\mathfrak{l},\ \mathfrak{l}_2)\dots(\mathfrak{l},\ \mathfrak{l}_l).$$

Da der Zähler des Ausdrucks rechter Hand in (41.) durch das Ideal $(\mathfrak{l}, \mathfrak{l}_1)$ teilbar ist, so ist derselbe als eine ganze Zahl in k auch durch $\mathfrak{l}_1$ teilbar. Entsprechend folgt die Teilbarkeit jenes Zählers durch $\mathfrak{l}_2, \dots, \mathfrak{l}_l$, und es ist derselbe also schliesslich auch durch l teilbar, d. h. die durch (41.) definirte Zahl ν ist auch jetzt eine ganze Zahl.

Durch Benutzung der Gleichung $t\Omega = \zeta^{-1}\Omega$ ergeben sich aus (41.) die beiden Formeln:

$$\begin{aligned} &\nu + t\nu + t^2\nu + \dots + t^{l-1}\nu = \pm 1, \\ (42.)\qquad &\nu + \zeta . t\nu + \zeta^2 . t^2\nu + \dots + \zeta^{l-1} . t^{l-1}\nu = \Omega. \end{aligned}$$

Eine Anwendung des Multiplicationssatzes der Determinanten, wie sie schon beim Beweise des Satzes 133 vorkam, ergiebt dann

$$N = \begin{vmatrix} \nu, & t\nu, & \dots, & t^{l-1}\nu \\ t^{l-1}\nu, & \nu, & \dots, & t^{l-2}\nu \\ \cdot & \cdot & \cdot & \cdot \\ t\nu, & t^2\nu, & \dots, & \nu \end{vmatrix} = \pm\,\Omega . s\Omega \dots s^{l-2}\,\Omega,$$

nnd hieraus folgt vermittelst der dritten in Satz 133 ausgesprochenen Eigenschaft der Zahl ω die Gleichung

$$N^l = \pm p^{\frac{l(l-1)}{2}}$$

und somit

$$\begin{vmatrix} \nu, & t\nu, & \dots, & t^{l-1}\nu \\ t^{l-1}\nu, & \nu, & \dots, & t^{l-2}\nu \\ \cdot & \cdot & \cdot & \cdot \\ t\nu, & t^2\nu, & \dots, & \nu \end{vmatrix}^2 = p^{l-1}.$$

Wir beweisen nun, dass die Discriminante des Körpers k notwendig $= p^{l-1}$ sein muss. In der That ist dieselbe wegen der letzten Gleichung ein positiver Teiler der Zahl p^{l-1}. Da sie nach Satz 44 oder nach Satz 94 nicht gleich 1 sein kann, so enthält sie die Primzahl p, und zwar nach den Bemerkungen zum Satze 79, notwendig in der $(l-1)$ten Potenz. Aus der soeben bewiesenen Thatsache folgt, dass $\nu, t\nu, \dots, t^{l-1}\nu$ eine Basis des Körpers k bilden; diese Basis ist offenbar eine Normalbasis. Die Zahl Ω ist wegen (42.) die aus dieser Normalbasis entspringende Wurzelzahl des Körpers k.

§ 108.

Die Zerlegung der $l$ten Potenz einer Wurzelzahl im Körper der $l$ten Einheitswurzeln.

Satz 135. Haben l, p, ζ, r, s die bisherige Bedeutung, und ist $k(\nu)$ ein Abel'scher Körper $l$ten Grades mit der Discriminante $d=p^{l-1}$ und Ω eine Wurzelzahl des Körpers $k(\nu)$, so gestattet die Zahl $\omega=\Omega^l$ im Körper $k(\zeta)$ die Zerlegung

$$\omega=\mathfrak{p}^{r_0+r_{-1}s+r_{-2}s^2+\cdots+r_{-l+2}s^{l-2}},$$

wo $\mathfrak{p}$ ein bestimmtes in p aufgehendes Primideal des Körpers $k(\zeta)$ bedeutet, und wo allgemein r_{-i} die kleinste positive ganze rationale Zahl bedeutet, welche der $-i$ten Potenz r^{-i} der Primitivzahl r nach l congruent ist. [*Kummer*[6, 11].]

Beweis. Die Primzahl p zerfällt im Körper $k(\zeta)$ in $l-1$ von einander verschiedene ideale Primfactoren $\mathfrak{p}, s\mathfrak{p}, \ldots, s^{l-2}\mathfrak{p}$; die Zahl ω muss durch jedes dieser Primideale teilbar sein. Denn nach dem Beweise zu Satz 134 ist die Relativdifferente des Körpers $k(\zeta, \Omega)$ in Bezug auf den Körper $k(\zeta)$ ein Teiler von $\Omega^l=\omega$; wäre nun ω etwa zu $\mathfrak{p}$ prim, so wäre also diese Relativdifferente und wegen Satz 41 auch die Differente und endlich wegen Satz 68 auch die Discriminante von $k(\zeta, \Omega)$ prim zu $\mathfrak{p}$, was nicht sein kann, da sie die Discriminante von $k(\nu)$ als Factor enthält. Wegen $n(\omega)=p^{\frac{l(l-1)}{2}}$ sind $\mathfrak{p}, s\mathfrak{p}, \ldots, s^{l-2}\mathfrak{p}$ zugleich die einzigen in ω aufgehenden Primideale. Es sei $\mathfrak{p}$ ein solcher unter diesen Primfactoren, welcher in der Zahl ω zu einer möglichst niedrigen Potenz vorkommt; dann haben wir

$$\omega=\mathfrak{p}^{a_0+a_1s+\cdots+a_{l-2}s^{l-2}},$$

wo $a_0, a_1, \ldots, a_{l-2}$ positive ganze rationale Zahlen bedeuten, unter welchen keine kleiner als a_0 ist. Die Bildung von $n(\omega)$ ergiebt

$$a_0+a_1+\cdots+a_{l-2}=\frac{l(l-1)}{2}.$$

Da $a_0, a_1, \ldots, a_{l-2}$ sämtlich >0 sind, können hiernach diese Zahlen nicht sämtlich durch l teilbar sein. Zufolge der ersten im Satze 133 bewiesenen Eigenschaft wird

$$\omega^{s-r}=\mathfrak{p}^{(s-r)(a_0+a_1s+\cdots+a_{l-2}s^{l-2})}=\alpha^l,$$

wo α eine Zahl in $k(\zeta)$ ist. Da die zu $\mathfrak{p}$ conjugirten Primideale sämtlich von $\mathfrak{p}$ und unter einander verschieden sind, so folgt hieraus, dass die ganzzahlige Function

$$(s-r)(a_0+a_1 s+\cdots+a_{l-2}s^{l-2})$$

der Veränderlichen s, wenn man nach Ausführung der Multiplication s^{l-1} durch 1 ersetzt, lauter durch l teilbare Coefficienten erhalten muss, d. h. diese Function ist $\equiv a_{l-2}(s^{l-1}-1)$ nach l. Daraus ist zunächst $a_{l-2}\not\equiv 0$ nach l ersichtlich, und wenn $a_{l-2}\equiv r^{m-l+2}$ nach l gesetzt wird, wo m eine der Zahlen $0, 1, \ldots, l-2$ bedeute, so folgt für jeden Index $i=0, 1, \ldots, l-2$ die Congruenz

$$a_i\equiv r^{m-i}, \quad (l).$$

Wir setzen allgemein $a_i=r_{m-i}+lb_i$ so, dass $0<r_{m-i}<l$ und b_i eine ganze rationale Zahl ist; dabei wird stets $b_i\geqq 0$. Da

$$r_m+r_{m-1}+\cdots+r_{m-l+2}=1+2+\cdots+(l-1)=\frac{l(l-1)}{2}$$

ist, so folgt $b_0+b_1+\cdots+b_{l-2}=0$, und daraus geht notwendig

$$b_0=0, \quad b_1=0, \quad \ldots, \quad b_{l-2}=0$$

hervor, d. h.

$$a_i=r_{m-i} \quad \text{für} \quad i=0, \quad 1, \quad \ldots, l-2.$$

Unter den Zahlen $r_0, r_1, \ldots, r_{l-2}$ ist offenbar $r_0=1$ die kleinste, und da a_0 unter den Coefficienten $a_0, a_1, \ldots, a_{l-2}$ möglichst klein sein sollte, so folgt $a_0=r_0=1$, d. h. $m=0$, und nunmehr allgemein $a_i=r_{-i}$, womit der Satz 135 bewiesen ist.

§ 109.

Eine Aequivalenz für die Primideale ersten Grades des Körpers der $l$ten Einheitswurzeln.

Aus den bisherigen Entwickelungen entnehmen wir eine wichtige Eigenschaft der in einer Primzahl $p\equiv 1$ nach l aufgehenden Primideale des Körpers der $l$ten Einheitswurzeln. Es gilt nämlich die Thatsache:

Satz 136. Es sei l eine ungerade Primzahl und $\zeta=e^{\frac{2i\pi}{l}}$, ferner r eine positive Primitivzahl nach l und $s=(\zeta:\zeta^r)$; wenn dann $\mathfrak{p}$ ein

beliebiges Primideal ersten Grades in dem Kreiskörper $k(\zeta)$ bedeutet, so besteht die Aequivalenz

$$\mathfrak{p}^{q_0+q_{-1}s+q_{-2}s^2+\cdots+q_{-l+2}s^{l-2}} \sim 1,$$

wo die Grössen q_{-i} ganze rationale, durch das Gleichungssystem

$$q_{-i} = \frac{rr_{-i}-r_{-i+1}}{l} \qquad (i=0,1,\ldots,l-2)$$

bestimmte, nicht negative Zahlen sind. Dabei haben $r_0, r_{-1}, \ldots, r_{-l+2}$ dieselbe Bedeutung wie in Satz 135, und es ist ausserdem $r_1 = r_{-l+2}$. [*Kummer*[6, 11].]

Beweis. Es mögen p und ω dieselbe Bedeutung wie in Satz 133 haben. Nach Satz 133 ist ω^{s-r} die $l$te Potenz einer Zahl α in $k(\zeta)$. Wenn wir für ω die in Satz 135 gegebene Darstellung durch $\mathfrak{p}$ einführen, so folgt

$$\mathfrak{p}^{(s-r)(r_0+r_{-1}s+\cdots+r_{-l+2}s^{l-2})} = \alpha^l,$$

und diese Gleichung zeigt, wenn wir daraus die Zerlegung von α selbst ermitteln, die Richtigkeit des Satzes 136.

Ist C eine beliebige Idealklasse des Kreiskörpers $k(\zeta)$ und $\mathfrak{j}$ ein Ideal in C, und bezeichnen wir mit $sC, s^2C, \ldots, s^{l-2}C$ bez. die durch $s\mathfrak{j}, s^2\mathfrak{j}, \ldots, s^{l-2}\mathfrak{j}$ bestimmten Idealklassen, so folgt mit Hülfe des Satzes 89 aus Satz 136 unmittelbar die Thatsache:

$$C^{q_0}(sC)^{q_{-1}}(s^2C)^{q_{-2}} \;\ldots\; (s^{l-2}C)^{q_{-l+2}} = 1.$$

§ 110.
Die Construction sämtlicher Normalbasen und Wurzelzahlen.

Die Sätze 133, 134 und 135 ermöglichen zunächst die Construction sämtlicher Wurzelzahlen des Abel'schen Körpers $k(\nu)$. Es gilt nämlich die Thatsache:

Satz 137. Bezeichnen $\boldsymbol{\Omega}$ und $\boldsymbol{\Omega}^*$ für den Abel'schen Körper k vom ungeraden Primzahlgrade l mit der Discriminante p^{l-1} zwei verschiedene, aber zu derselben erzeugenden Substitution t der Gruppe dieses Körpers gehörende Wurzelzahlen, so ist stets $\boldsymbol{\Omega}^* = \varepsilon\boldsymbol{\Omega}$, wo ε eine Einheit des Körpers $k(\zeta)$ bedeutet, welche die Congruenzeigenschaft $\varepsilon \equiv \pm 1$ nach $\mathfrak{l} = (1-\zeta)$ besitzt. Umgekehrt, wenn ε eine Einheit dieser Art in $k(\zeta)$ und $\boldsymbol{\Omega}$ für k irgend eine Wurzelzahl bezeichnet, so ist $\boldsymbol{\Omega}^* = \varepsilon\boldsymbol{\Omega}$ stets wiederum eine Wurzelzahl jenes Abel'schen Körpers k.

Beweis. Unter den Voraussetzungen in der ersten Aussage ist der Quotient $\varepsilon = \frac{\Omega^*}{\Omega}$ eine Zahl des aus k und $k(\zeta)$ zusammengesetzten Körpers, welche beim Uebergang von ζ, ν zu $\zeta, t\nu$ ungeändert bleibt und daher im Körper $k(\zeta)$ liegt. Für $\omega = \Omega^l$ werde der im Satze 135 enthaltene Ausdruck angenommen. Ist dann etwa $s^{-a}\,\mathfrak{p}$, wo a eine der Zahlen $0, 1, 2, \ldots, l-2$ bedeute, dasjenige unter den $l-1$ conjugirten, in p aufgehenden Primidealen des Körpers $k(\zeta)$, welches in $\omega^* = \Omega^{*l}$ nur zur ersten Potenz vorkommt, so hat man nach Satz 135 offenbar

$$\omega^* = \mathfrak{p}^{s^{-a}(r_0 + r_{-1}s + \cdots + r_{-l+2}s^{l-2})},$$

und hieraus folgt, dass das Primideal $\mathfrak{p}$ in ω^* genau zur r_{-a}ten Potenz vorkommt. Der Quotient $\frac{\omega^*}{\omega}$ kann daher in die Gestalt eines Bruches gebracht werden, dessen Zähler das Primideal $\mathfrak{p}$ in der $(r_{-a} - r_0)$ten Potenz enthält, während der Nenner zu $\mathfrak{p}$ prim ist. Da wegen $\frac{\omega^*}{\omega} = \varepsilon^l$ der Exponent $r_{-a} - r_0$ durch l teilbar sein muss, so folgt $r_{-a} = r_0$, d. h. $a = 0$. Wegen dieses Umstandes enthalten ω und ω^* die nämlichen Potenzen von Primidealen, und ε ist somit eine Einheit.

Die übrigen Behauptungen des Satzes 137 gehen unmittelbar aus den Sätzen 133 und 134 hervor.

Aus den zu t gehörenden Wurzelzahlen gewinnt man leicht nach Formel (41.) die sämtlichen Normalbasen $\nu, t\nu, \ldots, t^{l-1}\nu$ des Abel'schen Körpers k.

§ 111.

Die Lagrange'sche Normalbasis und die Lagrange'sche Wurzelzahl.

Es sei wieder l eine ungerade Primzahl, $\zeta = e^{\frac{2i\pi}{l}}$, ferner p eine rationale Primzahl von der Form $lm+1$, es werde $Z = e^{\frac{2i\pi}{p}}$ gesetzt, und es bezeichne R eine Primitivzahl nach p. Endlich bedeute k den Abel'schen Körper $l$ten Grades mit der Discriminante p^{l-1}.

Die $p-1$ Zahlen $Z, Z^2, \ldots, Z^{p-1}$ bilden eine Normalbasis des Körpers $k(Z)$; aus dem Beweise des Hülfssatzes 20 geht dann hervor,

dass die l Zahlen

$$\begin{aligned}
\lambda_0 &= Z + Z^{R^l} + Z^{R^{2l}} + \cdots + Z^{R^{(m-1)l}},\\
\lambda_1 &= Z^R + Z^{R^{1+l}} + Z^{R^{1+2l}} + \cdots + Z^{R^{1+(m-1)l}},\\
&\cdots\cdots\cdots\cdots\\
\lambda_{l-1} &= Z^{R^{l-1}} + Z^{R^{2l-1}} + Z^{R^{3l-1}} + \cdots + Z^{R^{ml-1}}
\end{aligned}$$

eine Normalbasis des Körpers k bilden. Aus dieser Normalbasis entspringt die folgende Wurzelzahl dieses Körpers:

$$\begin{aligned}
\varLambda &= \lambda_0 + \zeta\lambda_1 + \zeta^2\lambda_2 + \cdots + \zeta^{l-1}\lambda_{l-1},\\
&= Z + \zeta Z^R + \zeta^2 Z^{R^2} + \cdots + \zeta^{p-2} Z^{R^{p-2}}.
\end{aligned}$$

Diese besondere Normalbasis $\lambda_0, \lambda_1, \ldots, \lambda_{l-1}$ soll die **Lagrange'sche Normalbasis** und die besondere Wurzelzahl $\varLambda$ die **Lagrange'sche Wurzelzahl** heissen.

§ 112.

Die charakteristischen Eigenschaften der Lagrange'schen Wurzelzahl.

Die Lagrange'sche Wurzelzahl $\varLambda$ des Körpers k zeichnet sich vor den übrigen Wurzelzahlen von k durch folgende Eigenschaften aus:

Satz 138. Wenn die $l$te Potenz $\varLambda^l$ der Lagrange'schen Wurzelzahl $\varLambda$ gemäss Satz 135 durch die Formel

$$\varLambda^l = \mathfrak{p}^{r_0 + r_{-1}s + r_{-2}s^2 + \cdots + r_{-l+2}s^{l-2}}$$

dargestellt wird, so ist $\mathfrak{p}$ das durch die Formel

$$\mathfrak{p} = (p,\ \zeta - R^{-m}), \quad \left(m = \frac{p-1}{l}\right)$$

bestimmte Primideal; die Zeichen sind im übrigen wie in Satz 135 zu verstehen. Die Lagrange'sche Wurzelzahl $\varLambda$ ist $\equiv -1$ nach $\mathfrak{l}$ und hat ferner die Eigenschaft, dass ihr absoluter Betrag $= |\sqrt{p}|$ ist.

Umgekehrt, wenn einer Wurzelzahl Ω die letzteren Eigenschaften zukommen und ausserdem Ω^l gerade das soeben definirte Primideal $\mathfrak{p}$ zur ersten Potenz enthält, so ist $\Omega = \zeta^*\varLambda$, wo ζ^* eine $l$te Einheitswurzel bedeutet.

Beweis. Wird $\mathfrak{P} = (1-Z,\ \mathfrak{p})$ gesetzt, so erkennen wir mit Hülfe der Beziehungen $(1-Z)^{p-1} = (p)$ und $(p,\ \mathfrak{p}^{p-1}) = \mathfrak{p}$, dass

$$\mathfrak{P}^{p-1} = (p,\ (1-Z)^{p-2}\mathfrak{p},\ \ldots,\ \mathfrak{p}^{p-1}) = \mathfrak{p}.$$

wird; hieraus ist ersichtlich, dass $\mathfrak{P}$ in dem durch ζ und Z bestimmten Körper ein Primideal ist, und dass die Zahl $1-Z$ dieses Primideal $\mathfrak{P}$ nur zur ersten Potenz enthält. Setzen wir $Z=1+\Pi$ und berücksichtigen die Congruenz $\zeta\equiv R^{-m}$ nach $\mathfrak{p}$ und die Gleichung $(1+\Pi)^p=1$, so wird:

$$\Lambda \equiv \sum_{(x)} R^{-mx}(1+\Pi)^{R^x}, \quad (\mathfrak{p})$$

$$\equiv \sum_{(X)}\{X^{-m}\sum_{(Y)}\binom{X}{Y}\Pi^Y\}, \quad (\mathfrak{p}),$$

wo die bezüglichen Summen über $x=0, 1, 2, \ldots, p-2$; $X=1, 2, \ldots, p-1$, $Y=0, 1, 2, \ldots, X$ zu erstrecken sind. Aus der letzteren Formel gewinnen wir, wenn wir die Reihenfolge der Summationen umkehren, die Congruenz:

$$(43.) \qquad \Lambda \equiv -\frac{\Pi^m}{m!}, \quad (\mathfrak{P}^{m+1}).$$

Die Lagrange'sche Wurzelzahl Λ enthält also genau die $m$te Potenz von $\mathfrak{P}$ als Factor, und folglich ist Λ^l nur durch die erste Potenz von $\mathfrak{p}$ teilbar.

Bezeichnen wir die zu Λ conjugirt imaginäre Zahl mit $\overline{\Lambda}$, so ist

$$\overline{\Lambda} = Z^{-1}+\zeta^{-1}Z^{-R}+\zeta^{-2}Z^{-R^2}+\cdots+\zeta^{-p+2}Z^{-R^{p-2}};$$

dann wird, wenn wir im Product $\Lambda\overline{\Lambda}$ immer die je $p-1$ mit gleicher Potenz von ζ multiplicirten Glieder zusammennehmen,

$$\begin{aligned}\Lambda\overline{\Lambda} = &\quad (1 + 1 + \cdots + 1)\\ &+\zeta\,(Z^{R-1}+Z^{R^2-R}+\cdots+Z^{R^{p-1}-R^{p-2}})\\ &+\zeta^2(Z^{R^2-1}+Z^{R^3-R}+\cdots+Z^{R^p-R^{p-2}})\\ &\cdots\cdots\cdots\cdots\cdots\cdots\\ &+\zeta^{p-2}(Z^{R^{p-2}-1}+Z^{R^{p-1}-R}+\cdots+Z^{R^{2p-4}-R^{p-2}})\\ &= p-1-(\zeta+\zeta^2+\cdots+\zeta^{p-2}) = p.\end{aligned}$$

Damit ist der erste Teil des Satzes 138 vollständig bewiesen.

Der zweite Teil ist wesentlich die Umkehrung des ersten; die Richtigkeit des zweiten Teiles folgt ohne Mühe aus den Sätzen 135 und 137, wenn man überdies den Satz 48 heranzieht; man hat dabei zu beachten,

dass, wenn eine Zahl eines Abel'schen Zahlkörpers den absoluten Betrag 1 hat, diese Eigenschaft stets auch den zu ihr conjugirten Zahlen zukommt.

In entsprechender Weise wie die Congruenz (43.) können wir die sämtlichen folgenden Congruenzen ableiten [*Jacobi*[2]]:

$$(44.)\qquad s^{-i}\mathit{\Lambda} \equiv -\frac{\mathit{\Pi}^{r_{-i}m}}{(r_{-i}m)!}, \qquad \mathfrak{P}^{r_{-i}m+1}$$

für $i=0,\ 1,\ 2,\ \ldots,\ l-2$. Berücksichtigen wir die Thatsache, dass $\mathit{\Lambda}\equiv -1$ nach $\mathfrak{l}$ und $|\mathit{\Lambda}| = |\sqrt{p}|$ ist, so entspringt aus diesen Congruenzen (44.) ein anderer Beweis der Sätze 135 und 136. [*Kummer*[6, 11].]

Die sämtlichen Sätze und Beweise in diesem Capitel XXIV gelten entsprechend auch für $l=2$, nur dass dann die Discriminante des Abel'schen Körpers k den Wert $d=(-1)^{\frac{p-1}{2}}p$ bekommt.

Die Lagrange'sche Wurzelzahl $\mathit{\Lambda}$ des Körpers k ist eine ganze Zahl des aus $k(\zeta)$ und k zusammengesetzten Körpers, welche durch die in den Sätzen 133 und 138 aufgezählten Eigenschaften bis auf den Factor ζ^* völlig bestimmt ist. Um endlich auch diesen Factor ζ^* festzulegen, müsste man $\mathit{\Lambda} = |\sqrt{p}|\, e^{2i\pi\varphi}$ setzen derart, dass $0 \leqq \varphi < 1$ sei, und dann entscheiden, in welchem der l Intervalle

$$0 \leqq \varphi < \frac{1}{l}, \quad \frac{1}{l} \leqq \varphi < \frac{2}{l}, \quad \ldots, \quad \frac{l-1}{l} \leqq \varphi < 1$$

die betreffende Zahl φ gelegen ist. Aus dieser Frage entsteht in dem besonderen Falle, dass statt l die Primzahl 2 gewählt wird, das berühmte Problem der Bestimmung des Vorzeichens der Gauss'schen Summen. Vgl. § 124. Für den Fall $l=3$ werden wir auf eine von *Kummer* in Angriff genommene Aufgabe geführt. [*Kummer*[2, 4].]

Die Zahlen der Lagrange'schen Normalbasis werden gewöhnlich „Perioden" genannt. Die Litteratur weist eine Reihe von Abhandlungen auf, welche sich mit diesen Perioden, sowie mit verwandten ganzen Zahlen von Kreiskörpern beschäftigen. [*Kummer*[3, 17], *Fuchs*[1, 2], *Schwering*[1, 3, 4], *Kronecker*[17], *Smith*[1].] In der Litteratur finden sich noch Untersuchungen über besondere Kreiskörper [*Berkenbusch*[1], *Eisenstein*[10], *Schwering*[2], *Weber*[1, 2, 4], *Wolfskehl*[1]]. Auch sei hier erwähnt, dass, wenn die Primzahl $l < 100$ und nicht 29 oder 41 ist, der Kreiskörper $k(\zeta)$ stets eine solche Idealklasse enthält, deren Potenzen alle Klassen des Körpers liefern [*Kummer*[11, 13]].

Capitel XXV.

Das Reciprocitätsgesetz für $l$te Potenzreste zwischen einer rationalen Zahl und einer Zahl des Körpers der $l$ten Einheitswurzeln.

§ 113.

Der Potenzcharakter einer Zahl und das Symbol $\left\{\frac{\alpha}{\mathfrak{p}}\right\}$.

Es sei l eine ungerade Primzahl, $\zeta = e^{\frac{2i\pi}{l}}$, und $k(\zeta)$ bezeichne den durch ζ bestimmten Kreiskörper. Ist dann p eine rationale, von l verschiedene Primzahl und $\mathfrak{p}$ ein in p aufgehendes Primideal in $k(\zeta)$, und ist f der Grad von $\mathfrak{p}$, so gilt nach Satz 24 für jede nicht durch $\mathfrak{p}$ teilbare ganze Zahl α des Körpers $k(\zeta)$ die Congruenz

$$\alpha^{p^f-1} - 1 \equiv 0, \quad (\mathfrak{p}).$$

Da $p^f - 1$ nach Satz 119 durch l teilbar ist, so gestattet die linke Seite dieser Congruenz die Zerlegung

$$\alpha^{p^f-1} - 1 = \prod_{(c)} \left(\alpha^{\frac{p^f-1}{l}} - \zeta^c\right),$$

wo das Product über die Werte $c = 0, 1, \ldots, l-1$ zu erstrecken ist. Hieraus folgt, dass für einen und jedenfalls auch nur einen Wert c die Congruenz

$$\alpha^{\frac{p^f-1}{l}} \equiv \zeta^c, \quad (\mathfrak{p})$$

erfüllt ist. Man nennt die hier auftretende Einheitswurzel ζ^c den **Potenzcharakter der Zahl α in Bezug auf das Primideal** $\mathfrak{p}$ im Körper $k(\zeta)$ und bezeichnet diese Einheitswurzel ζ^c durch das **Symbol**

$$\left\{\frac{\alpha}{\mathfrak{p}}\right\},$$

so dass die Congruenz

$$(45.) \qquad \alpha^{\frac{p^f-1}{l}} \equiv \left\{\frac{\alpha}{\mathfrak{p}}\right\}, \quad (\mathfrak{p})$$

gilt. [*Kummer*[10].]

Sind α und β zwei durch $\mathfrak{p}$ nicht teilbare ganze Zahlen in $k(\zeta)$, so besteht, wie hieraus leicht ersichtlich, die Gleichung

$$\left\{\frac{\alpha\beta}{\mathfrak{p}}\right\} = \left\{\frac{\alpha}{\mathfrak{p}}\right\}\left\{\frac{\beta}{\mathfrak{p}}\right\}.$$

Wenn insbesondere die ganze Zahl α nach dem Primideal $\mathfrak{p}$ der $l$ten Potenz einer ganzen Zahl in $k(\zeta)$ congruent ist, so heisst α ein $l$ter **Potenzrest nach dem Primideal** $\mathfrak{p}$. Es gilt die Thatsache:

Satz 139. Bedeutet $\mathfrak{p}$ ein von $\mathfrak{l} = (1-\zeta)$ verschiedenes Primideal und α eine ganze zu $\mathfrak{p}$ prime Zahl in $k(\zeta)$, so ist α dann und nur dann $l$ter Potenzrest nach $\mathfrak{p}$, wenn $\left\{\frac{\alpha}{\mathfrak{p}}\right\} = 1$ ausfällt.

Beweis. Ist $\alpha \equiv \beta^l$ nach $\mathfrak{p}$, wo β wieder eine Zahl in $k(\zeta)$ bedeutet, so folgt $\alpha^{\frac{p^f-1}{l}} \equiv \beta^{p^f-1} \equiv 1$ nach $\mathfrak{p}$, d. h. $\left\{\frac{\alpha}{\mathfrak{p}}\right\} = 1$. Um die Umkehrung hiervon zu zeigen, bezeichnen wir mit ϱ eine Primitivzahl nach $\mathfrak{p}$ und setzen $\alpha \equiv \varrho^h$ nach $\mathfrak{p}$. Nehmen wir $\alpha^{\frac{p^f-1}{l}} \equiv \varrho^{\frac{h(p^f-1)}{l}} \equiv 1$ an, so folgt $\frac{h(p^f-1)}{l} \equiv 0$ nach p^f-1, d. h. h ist durch l teilbar, und folglich ist α ein $l$ter Potenzrest nach $\mathfrak{p}$, was zu beweisen war.

Für eine Primitivzahl ϱ nach $\mathfrak{p}$ ist der Potenzcharakter $\left\{\frac{\varrho}{\mathfrak{p}}\right\}$ sicherlich von 1 verschieden. Denn in der Reihe der Potenzen $\varrho, \varrho^2, \ldots$ ist ϱ^{p^f-1} die erste, welche $\equiv 1$ nach $\mathfrak{p}$ ausfällt, und also ist $\varrho^{\frac{p^f-1}{l}} \not\equiv 1$ nach $\mathfrak{p}$.

Es sei $\left\{\frac{\varrho}{\mathfrak{p}}\right\} = \zeta^g$; man bestimme eine zu p^f-1 prime ganze rationale Zahl g^* derart, dass $gg^* \equiv 1$ nach l wird; dann ist offenbar $\varrho^* = \varrho^{g^*}$ eine solche Primitivzahl nach $\mathfrak{p}$, für welche $\left\{\frac{\varrho^*}{\mathfrak{p}}\right\} = \zeta$ ausfällt. Ist nun α eine ganze, nicht durch $\mathfrak{p}$ teilbare Zahl in $k(\zeta)$, und hat man $\alpha \equiv \varrho^{*c}$ nach $\mathfrak{p}$, so besitzt α den Potenzcharakter ζ^c.

Hieraus ist leicht ersichtlich, dass das vollständige System der p^f-1 einander nach $\mathfrak{p}$ incongruenten Zahlen $1, \varrho^*, \varrho^{*2}, \ldots, \varrho^{*p^f-2}$ in l Teilsysteme zerfällt, von denen jedes $\frac{p^f-1}{l}$ Zahlen vom nämlichen Potenz-

charakter enthält. Insbesondere giebt es genau $\frac{p^f-1}{l}$ einander incongruente l te Potenzreste nach $\mathfrak{p}$.

Ist β eine ganze Zahl oder ein beliebiges Ideal und α eine zu β prime ganze Zahl in $k(\zeta)$, und wird $\beta = \mathfrak{p}\mathfrak{q}\ldots\mathfrak{w}$ gesetzt, wo $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{w}$ Primideale bedeuten, so werde das Symbol $\left\{\frac{\alpha}{\beta}\right\}$ durch die Gleichung

$$\left\{\frac{\alpha}{\beta}\right\} = \left\{\frac{\alpha}{\mathfrak{p}}\right\}\left\{\frac{\alpha}{\mathfrak{q}}\right\}\cdots\left\{\frac{\alpha}{\mathfrak{w}}\right\}$$

definirt.

§ 114.

Ein Hülfssatz über den Potenzcharakter der $l$ten Potenz der Lagrange'schen Wurzelzahl.

Es ist *Eisenstein* gelungen, dasjenige Reciprocitätsgesetz zu entdecken und zu beweisen, welches im Körper $k(\zeta)$ zwischen einer rationalen Zahl und einer beliebigen Zahl dieses Körpers besteht; dabei ist wieder $\zeta = e^{\frac{2i\pi}{l}}$ gesetzt, und l bedeutet eine ungerade Primzahl. Dieses Reciprocitätsgesetz ist zugleich ein bisher unentbehrliches Hülfsmittel zum Beweise des allgemeineren *Kummer*'schen Reciprocitätsgesetzes (vergl. Cap. XXXI). Dem Beweise des *Eisenstein*'schen Reciprocitätsgesetzes ist der folgende Hülfssatz vorauszuschicken:

Hülfssatz 21. Es sei $\zeta = e^{\frac{2i\pi}{l}}$; ferner bedeute p eine von l verschiedene rationale Primzahl von der Form $p = ml+1$, R eine Primitivzahl nach p und $\mathfrak{p}$ das Primideal ersten Grades in $k(\zeta)$:

$$\mathfrak{p} = (p,\ \zeta - R^{-m});$$

es werde $Z = e^{\frac{2i\pi}{p}}$, die Lagrange'sche Wurzelzahl

$$\Lambda = Z + \zeta Z^R + \zeta^2 Z^{R^2} + \cdots + \zeta^{p-2} Z^{R^{p-2}}$$

und $\pi = \Lambda^l$ gesetzt. Endlich bedeute q eine beliebige, von l und p verschiedene rationale Primzahl, $\mathfrak{q}$ ein in q aufgehendes Primideal des Körpers $k(\zeta)$ und g den Grad von $\mathfrak{q}$: dann drückt sich der Potenzcharakter der Zahl $\pi = \Lambda^l$ in Bezug auf das Ideal $\mathfrak{q}$ durch die

Formel aus

$$\left\{\frac{\pi}{\mathfrak{q}}\right\} = \left\{\frac{q}{\mathfrak{p}}\right\}^g.$$

Beweis. Durch g maliges Erheben in die q te Potenz folgt die Congruenz

(46.) $\quad \varLambda^{q^g} \equiv Z^{q^g} + \zeta^{q^g} Z^{Rq^g} + \zeta^{2q^g} Z^{R^2 q^g} + \cdots + \zeta^{(p-2)q^g} Z^{R^{p-2} q^g}, \quad (q).$

Berücksichtigen wir, dass dem Satze 119 zufolge $q^g \equiv 1$ nach l ist, und setzen $q^g \equiv R^h$ nach p, so wird die rechte Seite der Congruenz (46.)

$$Z^{R^h} + \zeta Z^{R^{h+1}} + \zeta^2 Z^{R^{h+2}} + \cdots + \zeta^{p-2} Z^{R^{h+p-2}} = \zeta^{-h} \varLambda.$$

Hieraus folgt, da $\varLambda$ wegen des Satzes 138 prim zu q ist, die Congruenz

$$\varLambda^{q^g - 1} \equiv \zeta^{-h}, \quad (q),$$

und also ist auch gewiss

$$\varLambda^{q^g - 1} = \pi^{\frac{q^g - 1}{l}} \equiv \zeta^{-h}, \quad (\mathfrak{q}),$$

d. h. es wird

(47.) $$\left\{\frac{\pi}{\mathfrak{q}}\right\} = \zeta^{-h}.$$

Andererseits entnimmt man aus den Congruenzen $q^g \equiv R^h$ nach p und $R^m \equiv \zeta^{-1}$ nach $\mathfrak{p}$ die Beziehungen:

$$q^{\frac{g(p-1)}{l}} = q^{gm} \equiv R^{hm} \equiv \zeta^{-h}, \quad (\mathfrak{p}),$$

d. h. es ist

(48.) $$\left\{\frac{q^g}{\mathfrak{p}}\right\} = \left\{\frac{q}{\mathfrak{p}}\right\}^g = \zeta^{-h};$$

die Gleichungen (47.) und (48.) zusammen ergeben den Hülfssatz 21.

§ 115.

Beweis des Reciprocitätsgesetzes im Körper $k(\zeta)$ zwischen einer rationalen und einer beliebigen Zahl.

Es bedeute $\mathfrak{l} = (1-\zeta)$ das in l aufgehende Primideal des Körpers $k(\zeta)$. Eine ganze Zahl α des Körpers $k(\zeta)$ heisse **semiprimär,** wenn sie zu $\mathfrak{l}$ prim und nach $\mathfrak{l}^2$ einer ganzen rationalen Zahl congruent ist.

Eine ganze rationale, nicht durch l teilbare Zahl ist hiernach stets semiprimär. Eine beliebige ganze, nicht durch $\mathfrak{l}$ teilbare Zahl α des Körpers $k(\zeta)$ kann durch Multiplication mit einer geeigneten Potenz der Einheitswurzel ζ stets in eine semiprimäre Zahl verwandelt werden. Ist nämlich

$$\alpha \equiv a + b(1-\zeta), \quad (\mathfrak{l}^2),$$

wo a und b ganze rationale Zahlen bedeuten, so ist

$$\zeta^{b^*}.\alpha \equiv a, \quad (\mathfrak{l}^2),$$

wenn b^* aus der Congruenz $ab^* \equiv b$ nach l bestimmt wird. Die Zahl $\zeta^{b^*}.\alpha$ ist mithin semiprimär.

Nach dieser Vorbemerkung lässt sich nunmehr das *Eisenstein*'sche Reciprocitätsgesetz, wie folgt, aussprechen:

Satz 140. Wenn a eine beliebige ganze rationale, nicht durch die ungerade Primzahl l teilbare Zahl und α eine beliebige semiprimäre und zu a prime ganze Zahl des Körpers $k(\zeta)$ der $l$ten Einheitswurzeln ist, so gilt in diesem Körper die Reciprocitätsgleichung

$$\left\{\frac{a}{\alpha}\right\} = \left\{\frac{\alpha}{a}\right\}.$$

[*Eisenstein*[2].]

Beweis. Wir verstehen unter r eine Primitivzahl nach l und schreiben $s = (\zeta : \zeta^r)$. Es werde zunächst angenommen, dass $a = q$ eine rationale Primzahl ist, und dass die Zahl α nur Primideale ersten Grades enthält. Es sei $\mathfrak{q}$ ein in q aufgehendes Primideal in $k(\zeta)$ und g der Grad von $\mathfrak{q}$, ferner sei p eine in der Norm $n(\alpha)$ vorkommende rationale Primzahl, und es mögen $\mathfrak{p}$ und π dazu die gleiche Bedeutung wie in Hülfssatz 21 haben. Ist nun s^u eine beliebige Potenz der Substitution s, und wenden wir den Hülfssatz 21 auf die Primideale $s^{-u}\mathfrak{q}$ und $\mathfrak{p}$ an, so ergiebt sich:

$$\left\{\frac{\pi}{s^{-u}\mathfrak{q}}\right\} = \left\{\frac{q}{\mathfrak{p}}\right\}^g.$$

Unterwerfen wir diese Gleichung der Substitution s^u, so folgt:

$$\left\{\frac{s^u \pi}{\mathfrak{q}}\right\} = \left\{\frac{q}{s^u \mathfrak{p}}\right\}^g. \tag{49.}$$

Die in der Norm $n(\alpha)$ vorkommenden, von einander verschiedenen rationalen Primzahlen seien $p = ml+1$, $p^* = m^*l+1$, ...; ferner mögen R, R^*, ... bez. Primitivzahlen nach p, p^*, ... bedeuten; end-

lich werde

$$\mathfrak{p} = (p,\ \zeta - R^{-m}), \quad \mathfrak{p}^* = (p^*,\ \zeta - R^{*-m^*}), \quad \ldots$$

gesetzt, und es gestatte die Zahl α die Zerlegung

$$\alpha = \mathfrak{p}^{F(s)} \mathfrak{p}^{*F^*(s)} \ldots,$$

wo die Exponenten F, F^*, ... ganzzahlige Functionen in s vom Grade $l-2$ mit lauter Coefficienten, die $\geqq 0$ sind, bedeuten.

Bezeichnen dann $\varLambda$, $\varLambda^*$, ... die bezüglichen, zu den Primzahlen p, p^*, ... und deren Primitivzahlen R, R^*, ... gehörigen Lagrange'schen Wurzelzahlen, und wird $\pi = \varLambda^l$, $\pi^* = \varLambda^{*l}$, ... gesetzt, so gelten nach Satz 138 die Zerlegungen:

$$\pi = \mathfrak{p}^{r_0 + r_{-1}s + r_{-2}s^2 + \cdots + r_{-l+2}s^{l-2}},$$

$$\pi^* = \mathfrak{p}^{*\,r_0 + r_{-1}s + r_{-2}s^2 + \cdots + r_{-l+2}s^{l-2}},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots,$$

wo r_{-h} die kleinste positive ganze rationale Zahl bedeutet, welche der $-h$ten Potenz r^{-h} der Primitivzahl r nach l congruent ist. Der Quotient

$$\varepsilon = \frac{\alpha^{r_0 + r_{-1}s + r_{-2}s^2 + \cdots + r_{-l+2}s^{l-2}}}{\pi^{F(s)} \pi^{*F^*(s)} \ldots}$$

ist daher offenbar eine Einheit des Körpers $k(\zeta)$. Wir wollen beweisen, dass diese Einheit $\varepsilon = \pm 1$ ist. Zu dem Zwecke bilden wir den Ausdruck

$$|\varepsilon|^2 = \varepsilon^{1+s^{\frac{l-1}{2}}} = \frac{\alpha^{\left(1+s^{\frac{l-1}{2}}\right)(r_0 + r_{-1}s + \cdots + r_{-l+2}s^{l-2})}}{(|\pi|^2)^{F(s)} (|\pi^*|^2)^{F^*(s)} \ldots}.$$

Wegen der für $h = 0, 1, 2, \ldots, \frac{l-3}{2}$ gültigen Gleichung

$$r_{-h} + r_{-h-\frac{l-1}{2}} = l$$

wird der Zähler des Bruches rechter Hand

$$\alpha^{\left(1+s^{\frac{l-1}{2}}\right)(r_0 + r_{-1}s + \cdots + r_{-l+2}s^{l-2})} = \alpha^{l(1+s+\cdots+s^{l-2})} = (n(\alpha))^l.$$

Berücksichtigen wir, dass nach Satz 138 $|\pi|^2 = p^l$, $|\pi^*|^2 = p^{*l}$, ... wird, so ergiebt sich $|\varepsilon| = 1$. Nach Satz 48 ist folglich ε bis auf einen Factor ± 1 eine Potenz der Einheitswurzel ζ. Da andererseits nach

Satz 138 die Congruenzen

$$\pi \equiv -1, \quad \pi^* \equiv -1, \quad \ldots, \quad \mathfrak{l}^l$$

bestehen, und daher π, π^*, ... sämtlich semiprimäre Zahlen sind, so ist auch ε eine semiprimäre Zahl; mithin wird $\varepsilon = \pm 1$, und es folgt demnach:

$$\alpha^{r_0 + r_{-1}s + \cdots + r_{-l+2}s^{l-2}} = \pm \pi^{F(s)} \pi^{*F^*(s)} \ldots$$

Diese Gleichung liefert unter Anwendung der Formel (49) die Reciprocitätsgleichung

$$(50.)\quad \left\{\frac{\alpha^{r_0 + r_{-1}s + \cdots + r_{-l+2}s^{l-2}}}{\mathfrak{q}}\right\} = \left\{\frac{q}{\mathfrak{p}^{F(s)}\mathfrak{p}^{*F^*(s)}\ldots}\right\}^g = \left\{\frac{q}{\alpha}\right\}^g.$$

Berücksichtigen wir, dass

$$\left\{\frac{s\alpha}{\mathfrak{q}}\right\} = \left\{\frac{\alpha}{s^{-1}\mathfrak{q}}\right\}^r, \quad \left\{\frac{s^2\alpha}{\mathfrak{q}}\right\} = \left\{\frac{\alpha}{s^{-2}\mathfrak{q}}\right\}^{r^2}, \quad \ldots$$

$$\ldots, \quad \left\{\frac{s^{l-2}\alpha}{\mathfrak{q}}\right\} = \left\{\frac{\alpha}{s^{-l+2}\mathfrak{q}}\right\}^{r^{l-2}}$$

ist, da ja die Symbole Potenzen von ζ darstellen, so folgt aus (50.) die Gleichung

$$\left\{\frac{\alpha}{q^g}\right\} = \left\{\frac{q}{\alpha}\right\}^g \quad \text{oder} \quad \left\{\frac{\alpha}{q}\right\} = \left\{\frac{q}{\alpha}\right\};$$

damit ist der Satz 140 unter den zunächst gemachten Einschränkungen, dass α nur Primideale ersten Grades enthält und α eine Primzahl ist, bewiesen.

Um die erstere Einschränkung zu beseitigen, nehmen wir jetzt an, es sei α eine beliebige semiprimäre, zu q prime ganze Zahl in $k(\zeta)$, welche auch Primideale von höherem als erstem Grade enthalten kann. Wir bilden dann die Zahl

$$\beta = \alpha^{\prod\limits_{(e)}(1-s^e)},$$

wo das im Exponenten stehende Product über sämtliche von $l-1$ verschiedene Teiler e der Zahl $l-1$ zu erstrecken ist, und setzen

$$\beta = \frac{\mathfrak{j}}{\mathfrak{k}}$$

in solcher Weise, dass $\mathfrak{j}$ und $\mathfrak{k}$ zu einander prime Ideale bedeuten; dieselben enthalten dann, wie leicht ersichtlich, nur Primideale ersten Grades als Factoren, und sie sind überdies nicht durch $\mathfrak{l}$ teilbar. Ist h die Anzahl der Idealklassen des Körpers $k(\zeta)$, so wird nach Satz 51 $\mathfrak{k}^h = (\varkappa)$,

wo $\varkappa$ eine ganze Zahl in $k(\zeta)$ bedeutet; setzen wir $\gamma = \beta\varkappa^l$, so wird auch γ eine ganze Zahl in $k(\zeta)$, welche nur Primideale ersten Grades als Primfactoren enthält, und überdies ist offenbar γ ebenso wie α semiprimär und zu q prim. Nach dem oben Bewiesenen ist daher

$$(51.)\qquad \left\{\frac{\gamma}{q}\right\} = \left\{\frac{q}{\gamma}\right\}.$$

Der einfacheren Darstellung halber wollen wir nun allgemein, wenn ϱ, σ zwei ganze zu q prime Zahlen in $k(\zeta)$ bedeuten,

$$\frac{\left\{\frac{\varrho}{q}\right\}}{\left\{\frac{\sigma}{q}\right\}} = \left\{\frac{\frac{\varrho}{\sigma}}{q}\right\} \quad \text{und} \quad \frac{\left\{\frac{q}{\varrho}\right\}}{\left\{\frac{q}{\sigma}\right\}} = \left\{\frac{q}{\frac{\varrho}{\sigma}}\right\}$$

schreiben, was zu keinem Widerspruche mit den bisherigen Festsetzungen führt; dann folgt wegen $\beta = \frac{\gamma}{\varkappa^l}$ aus (51.) offenbar die Gleichung

$$(52.)\qquad \left\{\frac{\beta}{q}\right\} = \left\{\frac{q}{\beta}\right\}.$$

Berücksichtigen wir die Gleichungen

$$\left\{\frac{s^u\alpha}{q}\right\} = \left\{\frac{\alpha}{q}\right\}^{r^u} \quad \text{und} \quad \left\{\frac{q}{s^u\alpha}\right\} = \left\{\frac{q}{\alpha}\right\}^{r^u},$$

so erkennen wir aus (52.), dass

$$\left\{\frac{\alpha}{q}\right\}^{\underset{(e)}{\Pi}(1-r^e)} = \left\{\frac{q}{\alpha}\right\}^{\underset{(e)}{\Pi}(1-r^e)}$$

wird. Wenn wir bedenken, dass das auf beiden Seiten als Exponent stehende Product nicht durch l teilbar ist, so ergiebt sich hieraus

$$\left\{\frac{\alpha}{q}\right\} = \left\{\frac{q}{\alpha}\right\}.$$

Wird endlich auch die ganze rationale durch l nicht teilbare Zahl a beliebig angenommen, nur so, dass a zu α prim ist, und wird $a = qq^* \ldots$ gesetzt, wo $q, q^*, \ldots$ rationale Primzahlen bedeuten, so folgt durch Multiplication der Gleichungen

$$\left\{\frac{q}{\alpha}\right\} = \left\{\frac{\alpha}{q}\right\}, \quad \left\{\frac{q^*}{\alpha}\right\} = \left\{\frac{\alpha}{q^*}\right\}, \quad \ldots$$

die Richtigkeit des Satzes 140 im allgemeinsten Falle.

Capitel XXVI.

Die Bestimmung der Anzahl der Idealklassen im Kreiskörper der $m$ten Einheitswurzeln.

§ 116.

Das Symbol $\left[\frac{a}{L}\right]$.

Um die in § 26 dargelegte transcendente Methode zur Bestimmung der Klassenanzahl eines Körpers auf den Fall des Kreiskörpers $k(e^{\frac{2i\pi}{m}})$, wo m irgend eine ganze rationale Zahl bedeutet, anzuwenden, definiren wir zunächst die folgenden **Symbole**:

Es sei l^h eine Potenz einer ungeraden Primzahl l mit positivem Exponenten und r eine Primitivzahl nach l^h. Ist dann a eine nicht durch l teilbare ganze rationale Zahl und a' dazu ein solcher Exponent, dass die Congruenz

$$r^{a'} \equiv a, \quad (l^h)$$

gilt, so definiren wir

$$\left[\frac{a}{l^h}\right] = e^{\frac{2i\pi a'}{l^{h-1}(l-1)}}.$$

Ferner setzen wir

$$\left[\frac{a}{l^h}\right] = 0,$$

sobald a durch l teilbar ist. Sind a, b zwei beliebige ganze rationale Zahlen, so wird dann offenbar

$$\left[\frac{ab}{l^h}\right] = \left[\frac{a}{l^h}\right]\left[\frac{b}{l^h}\right].$$

Des weiteren setzen wir, wenn a eine ungerade Zahl bedeutet, zunächst

$$\left[\frac{a}{2^2}\right] = (-1)^{\frac{a-1}{2}};$$

ferner für ein $h > 2$, wenn a' eine solche ganze rationale Zahl zu a ist, dass die Congruenz

$$5^{a'} \equiv \pm a, \quad (2^h)$$

gilt,

$$\left[\frac{a}{2^h}\right] = e^{\frac{2i\pi a'}{2^{h-2}}}.$$

Bedeutet endlich a eine gerade Zahl, so setzen wir

$$\left[\frac{a}{2^2}\right] = 0, \quad \left[\frac{a}{2^h}\right] = 0, \quad (h > 2).$$

Sind a, b irgend zwei ganze rationale Zahlen, so gelten dann, wie man sieht, die Gleichungen

$$\left[\frac{ab}{2^h}\right] = \left[\frac{a}{2^h}\right]\left[\frac{b}{2^h}\right], \quad (h > 1).$$

Durch diese Festsetzungen ist das Symbol $\left[\frac{a}{L}\right]$ vollständig für den Fall definirt, dass a eine beliebige ganze rationale Zahl und L eine höhere Potenz von 2 als die erste oder eine Potenz einer ungeraden Primzahl bedeutet, wobei im letzteren Falle irgend eine Primitivzahl r nach L von vorneherein zu Grunde zu legen ist.

Sind $l_1^{h_1}$, $l_2^{h_2}$, ... irgend welche fest gegebene Potenzen verschiedener ungerader Primzahlen und 2^{h^*} eine Potenz von 2, die grösser als 2^2 ist, so setzen wir zur Abkürzung

$$\left[\frac{a}{\underbrace{u_1, u_2, \ldots}}\right] = \left[\frac{a}{l_1^{h_1}}\right]^{u_1}\left[\frac{a}{l_2^{h_2}}\right]^{u_2}\cdots,$$

ferner

$$\left[\frac{a}{\underbrace{u; u_1, u_2, \ldots}}\right] = \left[\frac{a}{2^2}\right]^{u}\left[\frac{a}{l_1^{h_1}}\right]^{u_1}\left[\frac{a}{l_2^{h_2}}\right]^{u_2}\cdots,$$

ferner

$$\left[\frac{a}{\underbrace{u, u^*; u_1, u_2, \ldots}}\right] = \left[\frac{a}{2^2}\right]^{u}\left[\frac{a}{2^{h^*}}\right]^{u^*}\left[\frac{a}{l_1^{h_1}}\right]^{u_1}\left[\frac{a}{l_2^{h_2}}\right]^{u_2}\cdots;$$

darin soll a eine beliebige ganze rationale Zahl, und die Exponenten u, u^*; u_1, u_2, ... sollen ganze rationale, nicht negative Zahlen vorstellen. Endlich setzen wir fest, dass das Zeichen $\left[\frac{a}{L}\right]^0$ stets den Wert 1 bedeuten soll, auch wenn $\left[\frac{a}{L}\right] = 0$ ist.

§ 117.

Die Ausdrücke für die Klassenanzahl im Kreiskörper der $m$ten Einheitswurzeln.

Es gilt der folgende Satz, dessen Beweis in § 118 gegeben werden wird:

Satz 141. Es sei m eine ganze rationale positive Zahl von der Gestalt

$$m = l_1^{h_1} l_2^{h_2} \ldots, \quad \text{oder} \quad = 2^2 l_1^{h_1} l_2^{h_2} \ldots, \quad \text{oder} \quad = 2^{h^*} l_1^{h_1} l_2^{h_2} \ldots$$
$$(h^* > 2,\ h_1 > 0,\ h_2 > 0,\ \ldots),$$

wo $l_1, l_2, \ldots$ von einander verschiedene ungerade Primzahlen bedeuten. Es seien ferner $r_1, r_2, \ldots$ Primitivzahlen bez. nach $l_1^{h_1}, l_2^{h_2}, \ldots$ und mit ihrer Hülfe die betreffenden Symbole definirt. Dann kann die Klassenanzahl H des Kreiskörpers k der $m$ten Einheitswurzeln auf folgende zwei Weisen ausgedrückt werden:

Der erste Ausdruck für H lautet:

$$H = \frac{1}{\varkappa} \prod_{(u_1, u_2, \ldots)} \underset{s=1}{L} \prod_{(p)} \frac{1}{1 - \left[\overbrace{\frac{p}{u_1, u_2, \ldots}}\right] p^{-s}}$$

bez. entsteht aus dieser Formel, indem man $u_1, u_2, \ldots$ durch u; $u_1, u_2, \ldots$, bez. u, u^*; $u_1, u_2, \ldots$ ersetzt. Hierin ist dann das äussere Produkt Π über die Zahlen

$$(53.)\qquad \begin{cases} u_1 = 0,\ 1,\ \ldots,\ l_1^{h_1-1}(l_1-1)-1, \\ u_2 = 0,\ 1,\ \ldots,\ l_2^{h_2-1}(l_2-1)-1, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \text{ferner über} \\ u = 0,\ 1 \\ \text{und über} \\ u^* = 0,\ 1,\ \ldots,\ 2^{h^*-2}-1 \end{cases}$$

zu erstrecken mit Ausschluss der einen Wertverbindung $u_1 = 0$, $u_2 = 0$, ..., bez. $u = 0$; $u_1 = 0$, $u_2 = 0$, ..., bez. $u = 0$, $u^* = 0$; $u_1 = 0$, $u_2 = 0$, ...; es besteht daher nur aus einer endlichen Anzahl von Factoren. Jedes einzelne innere Product $\prod\limits_{(p)}$ soll über alle rationalen Primzahlen p erstreckt werden und ist mithin ein unendliches Product. Die Grösse $\varkappa$ ist die dem Körper k zugehörende Zahl des Satzes 56 (s. S. 229 unten).

Der zweite Ausdruck für H ist ein Product aus zwei in Bruchform erscheinenden Factoren und lautet:

$$H = \frac{\underset{(u_1, u_2, \ldots)}{\Pi} \underset{(n)}{\Sigma} \left[\overbrace{u_1, u_2, \ldots}^{n}\right] n}{(2m)^{\frac{1}{2}\Phi(m)-1}} \cdot \frac{\underset{(u_1, u_2, \ldots)}{\Pi} \underset{(n)}{\Sigma} \left[\overbrace{u_1, u_2, \ldots}^{n}\right] \log A_n}{R}$$

bez. entsteht aus dieser Formel, indem man zum ersten Bruch rechts den Factor $\frac{1}{2}$ hinzufügt und dann $u_1, u_2, \ldots$ durch u; $u_1, u_2, \ldots$ bez. u, u^*; $u_1, u_2, \ldots$ ersetzt. Hierin soll das Product Π im Zähler des ersten Bruches über alle diejenigen in (53.) angegebenen Werte erstreckt werden, für welche im ersten Falle $u_1+u_2+\cdots$ bez. in den zwei anderen Fällen $u+u_1+u_2+\cdots$ eine ungerade Zahl ist, während das Product Π im Zähler des zweiten Bruches über alle diejenigen in (53.) angegebenen Werte zu erstrecken ist, für welche im ersten Falle $u_1+u_2+\cdots$ bez. in den zwei anderen Fällen $u+u_1+u_2+\cdots$ eine gerade Zahl ist, mit Ausschluss immer der einen Wertverbindung $u_1=0$, $u_2=0, \ldots$, bez. $u=0$; $u_1=0$, $u_2=0, \ldots$, bez. $u=0$, $u^*=0$; $u_1=0$, $u_2=0, \ldots$. Weiter ist jede einzelne Summe $\underset{(n)}{\Sigma}$ in dem ersten Bruche über alle ganzen rationalen positiven Zahlen $n=1, 2, \ldots, m-1$, jede einzelne Summe $\underset{(n)}{\Sigma}$ in dem zweiten Bruche dagegen nur über alle diejenigen unter diesen Zahlen zu erstrecken, welche $<\frac{m}{2}$ sind. Endlich bedeutet $\log A_n$ den reellen Wert des Logarithmus der Kreiskörperzahl

$$A_n = \sqrt{(1-e^{\frac{2i\pi n}{m}})(1-e^{\frac{-2i\pi n}{m}})}$$

und R den Regulator des Kreiskörpers. [*Kummer*[22, 23].]

Die zwei Brüche im zweiten Ausdrucke für H hat *Kummer* den **ersten** und den **zweiten Factor der Klassenanzahl** genannt. Das Doppelte des ersten Factors einerseits und andererseits der zweite Factor der Klassenanzahl sind stets für sich ganze rationale Zahlen. [*Kronecker*[9].]

Auf Grund des zweiten Ausdrucks für H hat *Weber* bewiesen, dass die Klassenanzahl des Kreiskörpers der 2^{h^*}ten Einheitswurzeln stets eine ungerade Zahl ist. [*Weber*[1, 4].]

Der zweite Ausdruck für H gestattet noch weitere Umformungen. Im Falle, dass $m=l$ eine ungerade Primzahl ist, wird durch eine kleine Rechnung die Richtigkeit des folgenden Satzes erkannt:

Satz 142. Ist l eine ungerade Primzahl, so stellt sich die Klassenanzahl h des Kreiskörpers der $l$ten Einheitswurzeln, wie folgt, dar:

$$h = \frac{\prod\limits_{(u)} \sum\limits_{(n)} n e^{\frac{2 i \pi n' u}{l-1}}}{(2l)^{\frac{l-3}{2}}} \cdot \frac{\varDelta}{R}.$$

Hierin ist das Product $\prod\limits_{(u)}$ über die ungeraden Zahlen $u = 1, 3, 5, \ldots, l-2$ und jede einzelne Summe $\sum\limits_{(n)}$ über die Zahlen $n = 1, 2, 3, \ldots, l-1$ zu erstrecken; ferner ist eine Primitivzahl r nach l zu Grunde gelegt und man hat unter n' eine solche zu n gehörige ganze rationale Zahl zu verstehen, für welche $r^{n'} \equiv n$ nach l wird. $\varDelta$ bedeutet die Determinante

$$(-1)^{\frac{(l-3)(l-5)}{8}} \begin{vmatrix} \log \varepsilon_1, & \log \varepsilon_2, & \ldots, & \log \varepsilon_{\frac{l-3}{2}} \\ \log \varepsilon_2, & \log \varepsilon_3, & \ldots, & \log \varepsilon_{\frac{l-1}{2}} \\ \cdot & \cdot & \cdot & \cdot \\ \log \varepsilon_{\frac{l-3}{2}}, & \log \varepsilon_{\frac{l-1}{2}}, & \ldots & \log \varepsilon_{l-4} \end{vmatrix},$$

und dabei ist allgemein $\log \varepsilon_g$ der reelle Wert des Logarithmus der Einheit

$$\varepsilon_g = \sqrt{\frac{1-\zeta^{r^g}}{1-\zeta^{r^{g-1}}} \frac{1-\zeta^{-r^g}}{1-\zeta^{-r^{g-1}}}},$$

wo ζ für $e^{\frac{2i\pi}{l}}$ steht. [*Kummer*[7, 11], *Dedekind*[1].]

Die zwei Brüche hier in dem Ausdruck für h entstehen aus den zwei Brüchen in der oben gegebenen, auf den allgemeinen Fall bezüglichen Formel und sind also der erste und der zweite Factor der Klassenanzahl in dem früheren Sinne; im gegenwärtigen Falle sind beide Factoren der Klassenanzahl für sich ganze rationale Zahlen. Der zweite Factor stellt die Klassenanzahl des in $k(\zeta)$ enthaltenen reellen Unterkörpers vom $\frac{l-1}{2}$ten Grade dar. *Kummer* hat über diese zwei Factoren noch weitere Sätze aufgestellt, welche ihre Teilbarkeit durch 2 betreffen. [*Kummer*[25].] Der Versuch *Kronecker*'s, diese Sätze rein arithmetisch zu beweisen, weist einen Irrtum auf, und die von *Kronecker* gegebene Verallgemeinerung ist nicht richtig. [*Kronecker*[11].] Ausserdem hat

Kummer noch nach einer anderen Richtung hin Untersuchungen über die Bedeutung und die Eigenschaften dieser zwei Factoren angestellt. [*Kummer* [13].] Man vergleiche ferner Cap. XXXVI. Endlich hat *Kummer* den Satz behauptet, dass die Klassenanzahl eines jeden in $k(\zeta)$ enthaltenen Unterkörpers in der Klassenanzahl h des Körpers $k(\zeta)$ aufgeht. Der von ihm versuchte Beweis hiefür ist jedoch nicht stichhaltig. [*Kummer* [7].]

§ 118.

Die Ableitung der aufgestellten Ausdrücke für die Klassenanzahl des Kreiskörpers $k(e^{\frac{2i\pi}{m}})$.

Um den Satz 141 zu beweisen, fassen wir sogleich den complicirtesten Fall ins Auge, in welchem m durch 8 teilbar ist, und stellen den folgenden Hülfssatz auf:

Hülfssatz 22. Ist p eine beliebige rationale Primzahl und m eine durch 8 teilbare Zahl, so gilt unter Anwendung der in Satz 141 erklärten Bezeichnungen für reelle Werte $s > 1$ die Formel:

$$\prod_{(\mathfrak{P})}\{1-n(\mathfrak{P})^{-s}\} = \prod_{(u,u^*;u_1,u_2,\ldots)}\left\{1-\left[\frac{p}{u,\,u^*;\,u_1,\,u_2,\,\ldots}\right]p^{-s}\right\},$$

wo das Product linker Hand über alle verschiedenen Primideale $\mathfrak{P}$ des Kreiskörpers $k(e^{\frac{2i\pi}{m}})$ zu erstrecken ist, welche in der Primzahl p enthalten sind, und wo das Product rechter Hand über alle in (53.) angegebenen Wertsysteme $u, u^*; u_1, u_2, \ldots$ (das System $u=0$, $u^*=0$; $u_1=0$, $u_2=0, \ldots$ einbegriffen) genommen werden soll.

Beweis. Es sei zunächst p eine in m nicht aufgehende Primzahl; es sei l eine der ungeraden Primzahlen $l_1, l_2, \ldots$ und l^h die Potenz, zu der sie in m aufgeht, ferner r eine Primitivzahl nach l^h und $p \equiv r^{p'}$ nach l^h. Bedeutet e den grössten gemeinsamen Teiler der beiden Zahlen p' und $l^{h-1}(l-1)$ und wird $l^{h-1}(l-1)=ef$ gesetzt, so ist das Symbol $\left[\frac{p}{l^h}\right]$ offenbar genau eine $f$te und nicht eine niedere Einheitswurzel.

Wählen wir zunächst $l=l_1$ und setzen dementsprechend $h=h_1$, $e=e_1$, $l_1^{h_1-1}(l_1-1)=e_1f_1$, so folgt aus dem eben angegebenen Umstande die Formel:

$$\prod_{(u_1)}\left\{1-\left[\frac{p}{u,\,u^*;\,u_1,\,u_2,\,\ldots}\right]p^{-s}\right\} = \left\{1-\left[\frac{p}{u,\,u^*;\,u_2,\,u_3,\,\ldots}\right]^{f_1}p^{-sf_1}\right\}^{e_1},$$

wo das Product über die in (53.) bezeichneten Werte von u_1 zu erstrecken ist. Wählen wir ferner $l = l_2$ und setzen dementsprechend $h = h_2$, $e = e_2$, $l_2^{h_2-1}(l_2-1) = e_2 f_2$, so folgt, wenn f_{12} das kleinste gemeinsame Vielfache der Zahlen f_1, f_2 bezeichnet:

$$\underset{(u_1, u_2)}{\Pi}\left\{1-\left[\frac{p}{u,\ u^*;\ u_1,\ u_2,\ \ldots}\right]p^{-s}\right\}$$

$$= \left\{1-\left[\frac{p}{u,\ u^*;\ u_3,\ u_4,\ \ldots}\right]^{f_{12}} p^{-sf_{12}}\right\}^{\frac{e_1 e_2 f_1 f_2}{f_{12}}},$$

wo das Product sich über die in (53.) bezeichneten Werte von u_1, u_2 erstreckt, und ebenso wird weiterhin, wenn $f_{12\ldots}$ das kleinste gemeinsame Vielfache der Zahlen f_1, f_2, ... bezeichnet:

$$\underset{(u_1, u_2, \ldots)}{\Pi}\left\{1-\left[\frac{p}{u,\ u^*;\ u_1,\ u_2,\ \ldots}\right]p^{-s}\right\}$$

$$= \left\{1-\left[\frac{p}{u,\ u^*}\right]^{f_{12\ldots}} p^{-sf_{12\ldots}}\right\}^{\frac{e_1 e_2 \ldots f_1 f_2 \ldots}{f_{12\ldots}}},$$

wo das Product über alle in (53.) bezeichneten Werte u_1, u_2, ... zu erstrecken ist.

Es sei ferner $p \equiv \pm 5^{p'}$ nach 2^{h^*}, es bedeute e^* den grössten gemeinsamen Teiler der Zahlen p' und 2^{h^*-2}, und es werde $2^{h^*-2} = e^* f^*$ gesetzt; dann ist offenbar $\left[\frac{p}{2^{h^*}}\right]$ genau eine f^*te und nicht eine niedere Einheitswurzel. Wir erhalten infolge dessen, wenn $f^*_{12\ldots}$ das kleinste gemeinsame Vielfache der Zahlen f^*, f_1, f_2, ... bezeichnet:

$$\underset{(u^*;\, u_1, u_2, \ldots)}{\Pi}\left\{1-\left[\frac{p}{u,\ u^*;\ u_1,\ u_2,\ \ldots}\right]p^{-s}\right\}$$

$$= \left\{1-\left[\frac{p}{2^2}\right]^{uf^*_{12\ldots}} p^{-sf^*_{12\ldots}}\right\}^{\frac{e^* e_1 e_2 \ldots f^* f_1 f_2 \ldots}{f^*_{12\ldots}}},$$

wo nun das Product auch über die in (53.) bezeichneten Werte von u^* zu nehmen ist.

Endlich sei $\bar{e}$ der grösste gemeinsame Teiler von $\frac{p-1}{2}$ und 2, und man setze $2 = \bar{e}\bar{f}$; aus der letzten Formel folgt dann, wenn F das kleinste gemeinsame Vielfache der Zahlen $\bar{e}$, e^*, e_1, e_2, ... bezeichnet und zur

Abkürzung

$$E = \frac{\bar{e}e^* e_1 e_2 \ldots \bar{f} f^* f_1 f_2 \ldots}{F}$$

gesetzt wird,

$$(54.)\quad \prod_{(u,\, u^*;\, u_1,\, u_2, \ldots)} \left\{1 - \left[\overbrace{\qquad\qquad}^{p}_{u,\; u^*;\; u_1,\; u_2,\; \ldots}\right] p^{-s}\right\} = \{1 - p^{-sF}\}^E,$$

wo das Product sich über alle in (53.) bezeichneten Wertverbindungen $u, u^*; u_1, u_2, \ldots$ erstreckt. Man sieht sofort, dass F der kleinste positive Exponent mit der Congruenzeigenschaft $p^F \equiv 1$ nach m ist. Da ferner $FE = \Phi(m)$ ist, so folgt aus (54.) mit Rücksicht auf den Satz 125 die im Hülfssatz 22 aufgestellte Formel. Mit Hülfe der zweiten Aussage in Satz 125 erkennt man dann leicht die Gültigkeit dieser Formel auch in dem Falle, dass p eine in m enthaltene Primzahl ist.

Die Richtigkeit des ersten in Satz 141 aufgestellten Ausdruckes für H erkennen wir nun unmittelbar auf Grund des Satzes 56, wenn wir die zweite in § 27 gegebene Darstellung von $\zeta(s)$ und den eben bewiesenen Hülfssatz 22 anwenden.

Zur Ableitung des zweiten Ausdruckes für H formen wir zunächst das im ersten Ausdrucke hinter dem Limes-Zeichen stehende Product in eine unendliche Summe, wie folgt, um:

$$\prod_{(p)} \frac{1}{1 - \left[\overbrace{\qquad\qquad}^{p}_{u,\; u^*;\; u_1,\; u_2,\; \ldots}\right] p^{-s}} = \sum_{(n=1,2,3,\ldots)} \left[\overbrace{\qquad\qquad}^{n}_{u,\; u^*;\; u_1,\; u_2,\; \ldots}\right] \frac{1}{n^s}.$$

Die weitere Behandlung der rechts stehenden Summe geschieht dann am einfachsten, indem wir in derselben

$$\frac{1}{n^s} = \frac{1}{\Gamma(s)} \int_0^\infty \mathrm{e}^{-nt} t^{s-1}\, dt$$

einsetzen und dann in entsprechender Weise verfahren wie in § 86.

§ 119.

Das Vorhandensein von unendlich vielen rationalen Primzahlen, welche nach einer gegebenen Zahl einen vorgeschriebenen, zu ihr primen Rest lassen.

Jeder der zwei in § 117 aufgestellten und soeben bewiesenen Ausdrücke für die Klassenanzahl H des Kreiskörpers der $m$ten Einheitswurzeln gestattet eine wichtige Folgerung. Der erstere Ausdruck nämlich kann zum Nachweis der folgenden Thatsache dienen:

Satz 143. *Bedeuten m und n zwei zu einander prime ganze rationale Zahlen, so giebt es stets unendlich viele rationale Primzahlen p mit der Congruenzeigenschaft $p \equiv n$ nach m. [Dirichlet[5, 6], Dedekind[1].]*

Beweis. Auch hier betrachten wir nur den complicirtesten Fall, wo m durch 8 teilbar ist, und setzen, wie in § 117, $m = 2^{h^*} l_1^{h_1} l_2^{h_2} \dots$. Jedes der dort betrachteten unendlichen Producte

$$\prod_{(p)} \frac{1}{1 - \left[\overbrace{u,\, u^*;\; u_1,\, u_2,\, \dots}^{p}\right] p^{-s}}$$

mit Ausschluss desjenigen, welches der Wertverbindung $u = 0$, $u^* = 0$; $u_1 = 0$, $u_2 = 0$, ... entspricht, convergirt für $s = 1$ nach einem bestimmten Grenzwerte; aus der ersten in § 117 gegebenen Darstellung der Klassenanzahl H folgt, dass diese Grenzwerte sämtlich von 0 verschieden ausfallen; wir können daher die Logarithmen dieser Producte verwenden, und es führen dann entsprechende einfache Betrachtungen, wie sie in § 80 angestellt worden sind, zu dem Resultate, dass für jedes betrachtete Wertsystem $u, u^*; u_1, u_2, \dots$, immer von dem einen Systeme $u = 0, u^* = 0; u_1 = 0, u_2 = 0, \dots$ abgesehen, die unendliche Summe

$$(55.) \qquad \sum_{(p)} \left[\overbrace{u,\, u^*;\; u_1,\, u_2,\, \dots}^{p}\right] \frac{1}{p^s},$$

wo p alle rationalen Primzahlen durchläuft, in der Grenze für $s = 1$ stets endlich bleibt.

Da n zu m prim vorausgesetzt ist, so sind die Symbole

$$\left[\frac{n}{2^2}\right], \quad \left[\frac{n}{2^h}\right], \quad \left[\frac{n}{l_1^{h_1}}\right], \quad \left[\frac{n}{l_2^{h_2}}\right],$$

sämtlich von 0 verschieden. Wir multipliciren den Ausdruck (55.) mit

$$\frac{1}{\left[\frac{n}{2^2}\right]^u \left[\frac{n}{2^{h^*}}\right]^{u^*} \left[\frac{n}{l_1^{h_1}}\right]^{u_1} \left[\frac{n}{l_2^{h_2}}\right]^{u_2} \cdots},$$

lassen dann $u, u^*; u_1, u_2, \dots$ alle in (53.) angegebenen Werte durchlaufen, doch so, dass das eine System $u = 0, u^* = 0; u_1 = 0, u_2 = 0, \dots$ ausgeschlossen wird, und addiren sämtliche so entstehenden Ausdrücke zu der unendlichen Summe (26.) (siehe § 80, S. 311). Auf diese Weise

geht der Ausdruck

$$(56.)\quad \begin{cases} \sum_{(p)}(1+P)(1+P^*+P^{*2}+\cdots+P^{*2^{h^*-2}-1})\cdot \\ \qquad (1+P_1+P_1^2+\cdots+P_1^{l_1^{h_1-1}(l_1-1)-1})\cdot \\ \qquad (1+P_2+P_2^2+\cdots+P_2^{l_2^{h_2-1}(l_2-1)-1})\cdots\frac{1}{p^s}, \end{cases}$$

hervor, wo zur Abkürzung

$$P=\frac{\left[\frac{p}{2^2}\right]}{\left[\frac{n}{2^2}\right]},\quad P^*=\frac{\left[\frac{p}{2^{h^*}}\right]}{\left[\frac{n}{2^{h^*}}\right]},\quad P_1=\frac{\left[\frac{p}{l_1^{h_1}}\right]}{\left[\frac{n}{l_1^{h_1}}\right]},\quad P_2=\frac{\left[\frac{p}{l_2^{h_2}}\right]}{\left[\frac{n}{l_2^{h_2}}\right]},\ldots$$

gesetzt ist. Sehen wir in dieser unendlichen Reihe (56.) von denjenigen Gliedern ab, die den in m aufgehenden Primzahlen 2, l_1, l_2, ... entsprechen, und die nur in endlicher Anzahl vorhanden sind, so ist im übrigen diese Reihe gleich $\Phi(m)\sum\frac{1}{p^s}$, wo p nur alle diejenigen rationalen Primzahlen durchläuft, für welche die Werte P, P^*, P_1, P_2, ... sämtlich gleich 1 werden, d. s. eben die Primzahlen, welche der im Satze 143 verlangten Congruenzbedingung genügen.

Da die unendliche Summe (26.) (s. S. 311) für $s=1$ über alle Grenzen wächst, dagegen die hier betrachteten Reihen (55.) für $s=1$ sämtlich endlich bleiben, so folgt, dass auch der Wert der unendlichen Reihe (56.) für $s=1$ über alle Grenzen wächst, d. h. die Primzahlen mit der verlangten Congruenzeigenschaft sind notwendig in unendlicher Anzahl vorhanden.

§ 120.

Die Darstellung sämtlicher Einheiten des Kreiskörpers durch die Kreiseinheiten.

Der zweite der beiden in § 117 aufgestellten Ausdrücke kann zum Nachweise des folgenden Satzes dienen:

Satz 144. *Jede Einheit eines Abel'schen Körpers ist eine Wurzel mit rationalem ganzzahligem Exponenten aus einem Product von Kreiseinheiten.*

Beweis. Fassen wir zunächst den Fall ins Auge, dass $m=l$ eine ungerade Primzahl ist. Nach der Formel im Satze 142 enthält der zweite Factor der Klassenanzahl im Zähler eine gewisse Determinante Δ;

jene Determinante Δ ist daher notwendig von 0 verschieden, und hieraus folgt mit Rücksicht auf die in § 20 und § 21 angestellten Betrachtungen, dass die in Satz 142 angegebenen $\frac{l-3}{2}$ Einheiten $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\frac{l-3}{2}}$ des Kreiskörpers $k(e^{\frac{2i\pi}{l}})$ ein System von unabhängigen Einheiten bilden. Dieser Umstand lehrt die Richtigkeit des Satzes 144 für den besonderen Fall des Kreiskörpers $k(e^{\frac{2i\pi}{l}})$, sowie auch für alle in diesem Körper enthaltenen Unterkörper. [*Kummer*[11].]

Eine ähnliche Umformung des zweiten Factors der Klassenanzahl, wie sie in Satz 142 gegeben wird, ist auch im Falle des Kreiskörpers der $m$ten Einheitswurzeln möglich, wenn m eine beliebige zusammengesetzte Zahl ist; der betreffende Ausdruck ermöglicht dann auf Grund des Satzes 131 den allgemeinen Beweis des Satzes 144.

Ein reiches Zahlenmaterial, welches zu tieferen Untersuchungen in der Theorie der Kreiskörpers von hohem Nutzen ist, bieten die von *Reuschle* berechneten Tafeln complexer Primzahlen. [*Reuschle*[1], *Kummer*[24], *Kronecker*[12].]

Capitel XXVII.

Anwendungen der Theorie des Kreiskörpers auf den quadratischen Körper.

§ 121.

Die Erzeugung der Einheiten des reellen quadratischen Körpers aus Kreiseinheiten.

Indem wir gewisse in den vorangehenden Capiteln abgeleitete Eigenschaften des Kreiskörpers der $m$ten Einheitswurzeln für einen in ihm enthaltenen quadratischen Unterkörper verwerten, gelangen wir zu neuen Sätzen über den quadratischen Zahlkörper. Die Fruchtbarkeit dieser Methode wird noch erhöht, wenn wir sie mit denjenigen Wahrheiten in Verbindung bringen, welche im dritten Teil dieses Berichtes durch unmittelbare Betrachtung des quadratischen Körpers gewonnen worden sind.

Nach dem allgemeinen Satze 144 ist insbesondere eine jede Einheit eines reellen quadratischen Körpers $k(\sqrt{m})$ eine Wurzel mit rationalem

ganzzahligem Exponenten aus einem Producte von Kreiseinheiten; es wird eine specielle Einheit des Körpers $k(\sqrt{m})$ einfach durch den folgenden Ausdruck

$$\frac{\prod\limits_{(b)}\left(e^{\frac{bi\pi}{d}}-e^{-\frac{bi\pi}{d}}\right)}{\prod\limits_{(a)}\left(e^{\frac{ai\pi}{d}}-e^{-\frac{ai\pi}{d}}\right)}$$

erhalten, wo d die Discriminante des Körpers $k(\sqrt{m})$ bedeutet, und wo die Producte $\prod\limits_{(a)}$, $\prod\limits_{(b)}$ über alle diejenigen Zahlen a oder b der Reihe $1, 2, \ldots, d$ zu erstrecken sind, welche der Bedingung $\left(\frac{d}{a}\right)=+1$ bez. $\left(\frac{d}{b}\right)=-1$ genügen. [*Dirichlet*[7].] Vgl. § 86.

§ 122.

Das Reciprocitätsgesetz für quadratische Reste.

Es sei l eine ungerade rationale Primzahl, r eine Primitivzahl nach l; ferner $\zeta = e^{\frac{2i\pi}{l}}$ und $s = (\zeta : \zeta^r)$. Zu der aus den $\frac{l-1}{2}$ Substitutionen $1, s^2, s^4, \ldots s^{l-3}$ gebildeten Untergruppe der Gruppe des Kreiskörpers $k(\zeta)$ gehört ein gewisser quadratischer Unterkörper k^* des Kreiskörpers $k(\zeta)$. Da die Discriminante des Körpers $k(\zeta)$ nach Satz 118 gleich $(-1)^{\frac{l-1}{2}}\, l^{l-2}$ ist, so enthält nach Satz 39 die Discriminante von k^* keine andere rationale Primzahl als l und besitzt daher wegen Satz 95 den Wert $d = (-1)^{\frac{l-1}{2}}\, l$.

Es sei p entweder die Primzahl 2 oder eine beliebige von l verschiedene ungerade rationale Primzahl. Indem wir die Zerlegung von p einerseits in dem Kreiskörper $k(\zeta)$ der $l$ten Einheitswurzeln, andererseits direct nach Satz 97 in dem quadratischen Unterkörper k^* ausführen und hernach die erhaltenen Resultate mit einander vergleichen, gelangen wir zu einem neuen Beweise des Reciprocitätsgesetzes für quadratische Reste. [*Kronecker*[15].] Wir verfahren dabei, wie folgt:

Ist f der kleinste positive Exponent, für welchen $p^f \equiv 1$ nach l ausfällt, und wird $e = \frac{l-1}{f}$ gesetzt, so zerlegt sich nach Satz 119 die Primzahl p im Körper $k(\zeta)$ in e Primideale $\mathfrak{P}, s\mathfrak{P}, \ldots, s^{e-1}\mathfrak{P}$, und

es ist der gemeinsame Zerlegungskörper k_z dieser Primideale nach Satz 129 vom Grade e. Die rationale Primzahl p ist alsdann offenbar in dem quadratischen Körper k^* zerlegbar oder nicht zerlegbar, je nachdem der Körper k^* in k_z als Unterkörper enthalten ist oder nicht. Bedenken wir, dass der Körper $k(\zeta)$ nur den einen quadratischen Unterkörper k^* enthält, und ferner, dass ein Abel'scher Körper dann und nur dann überhaupt einen quadratischen Unterkörper besitzt, wenn sein Grad gerade ist, so folgt, dass k^* dann und nur dann in k_z enthalten ist, wenn die Zahl e gerade ausfällt. Andererseits ist nach Satz 97 die Primzahl p in k^* zerlegbar oder nicht zerlegbar, je nachdem $\left(\frac{(-1)^{\frac{l-1}{2}}l}{p}\right)=+1$ oder $=-1$ ist. Ist nun e gerade, so folgt $p^{\frac{l-1}{2}}=p^{f\cdot\frac{e}{2}}\equiv 1$ nach l, d. h. $\left(\frac{p}{l}\right)=+1$; im anderen Falle wird $p^{\frac{l-1}{2}}=p^{\frac{f}{2}\cdot e}\equiv(-1)^e\equiv -1$ nach l, d. h. $\left(\frac{p}{l}\right)=-1$. Es ist mithin in jedem Falle

$$(57.)\qquad \left(\frac{p}{l}\right)=\left(\frac{(-1)^{\frac{l-1}{2}}l}{p}\right).$$

Wir nehmen zunächst p ungerade an; aus (57.) folgt

$$(58.)\qquad \left(\frac{l}{p}\right)\left(\frac{p}{l}\right)=\left(\frac{(-1)^{\frac{l-1}{2}}}{p}\right)$$

und weiter, wenn wir p und l mit einander vertauschen,

$$\left(\frac{(-1)^{\frac{l-1}{2}}}{p}\right)=\left(\frac{(-1)^{\frac{p-1}{2}}}{l}\right).$$

Die letztere Formel ergiebt, wenn wir $l=3$ nehmen,

$$(59.)\qquad \left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}.$$

Die Verbindung der Gleichung (59.) mit (58.) liefert

$$(60.)\qquad \left(\frac{l}{p}\right)\left(\frac{p}{l}\right)=(-1)^{\frac{l-1}{2}\cdot\frac{p-1}{2}}.$$

Setzen wir in (57.) $p=2$, so folgt

$$(61.)\qquad \left(\frac{2}{l}\right)=\left(\frac{(-1)^{\frac{l-1}{2}}l}{2}\right)=(-1)^{\frac{l^2-1}{8}}.$$

Die Formeln (60.), (59.) und (61.) enthalten das Reciprocitätsgesetz für quadratische Reste nebst den zugehörigen Ergänzungssätzen.

§ 123.

Der imaginäre quadratische Körper mit einer Primzahldiscriminante.

Satz 145. Wenn l eine rationale Primzahl mit der Congruenzeigenschaft $l\equiv 3$ nach 4 ist und p eine rationale Primzahl von der Gestalt $p=ml+1$ bedeutet, so gilt für ein jedes in p aufgehende Primideal $\mathfrak{p}$ des imaginären quadratischen Körpers $k(\sqrt{-l})$ die Aequivalenz

$$\mathfrak{p}^{\frac{\Sigma b-\Sigma a}{l}}\sim 1,$$

wo Σa die Summe der kleinsten positiven quadratischen Reste und Σb die Summe der kleinsten positiven quadratischen Nichtreste nach l bedeutet.

Setzt man ferner $p=\mathfrak{p}\mathfrak{p}'$ und

$$\mathfrak{p}^{\frac{\Sigma b-\Sigma a}{l}}=(\pi),$$

wobei π eine ganze Zahl des imaginären quadratischen Körpers $k(\sqrt{-l})$ bedeutet, so gilt die Congruenz

$$\pi\equiv\pm\frac{1}{\prod\limits_{(a)}(am)!},\quad (\mathfrak{p}'),$$

wo das im Nenner stehende Product über alle kleinsten positiven quadratischen Reste a nach l zu erstrecken ist. [*Jacobi*[1,2,3,4], *Cauchy*[1], *Eisenstein*[4].]

Beweis. Nach Satz 136 kann man, wenn $\mathfrak{P}$ ein Primideal ersten Grades in $k(\zeta)$ bedeutet, unter Benutzung der dort erklärten Bezeichnungen

$$(62.)\qquad \mathfrak{P}^{q_0+q_{-1}s+q_{-2}s^2+\cdots+q_{-l+2}s^{l-2}}=(A)$$

setzen derart, dass A eine ganze Zahl in $k(\zeta)$ ist. Ist dann $p=ml+1$ die durch $\mathfrak{P}$ teilbare rationale Primzahl und $p=\mathfrak{p}\mathfrak{p}'$ die Zerlegung dieser Primzahl in dem in $k(\zeta)$ enthaltenen quadratischen Unterkörper $k(\sqrt{-l})$,

so gehen andererseits diese zwei Primideale $\mathfrak{p}$ und $\mathfrak{p}'$ des Körpers $k(\sqrt{-l})$ in der Gestalt hervor:

$$\mathfrak{p} = \mathfrak{P}^{1+s^2+s^4+\cdots+s^{l-3}},$$
$$\mathfrak{p}' = s\mathfrak{p} = \mathfrak{P}^{s(1+s^2+s^4+\cdots+s^{l-3})}.$$

Wenn wir die Gleichung (62.) in die $(1+s^2+s^4+\cdots+s^{l-3})$te symbolische Potenz erheben, so folgt

$$\mathfrak{p}^{q_0+q_{-2}+q_{-4}+\cdots+q_{-l+3}}\mathfrak{p}'^{q_{-1}+q_{-3}+q_{-5}+\cdots+q_{-l+2}} = (\alpha),$$

wo α eine Zahl in $k(\sqrt{-l})$ bedeutet. Wegen

$$q_{-1}+q_{-3}+\cdots+q_{-l+2}-q_0-q_{-2}-\cdots-q_{-l+3} = (r+1)\frac{\Sigma b-\Sigma a}{l}$$

folgt, wenn wir die Aequivalenz $\mathfrak{p}\mathfrak{p}' \sim 1$ berücksichtigen,

$$(63.)\qquad \mathfrak{p}^{(r+1)\frac{\Sigma b-\Sigma a}{l}} \sim 1.$$

Andererseits kann man nach Satz 135

$$\mathfrak{P}^{r_0+r_{-1}s+r_{-2}s^2+\cdots+r_{-l+2}s^{l-2}} = (B)$$

setzen, derart, dass B eine ganze Zahl in $k(\zeta)$ bedeutet. Wenn wir diese Gleichung in die $(1+s^2+s^4+\cdots+s^{l-3})$te symbolische Potenz erheben, so folgt

$$(64.)\qquad \mathfrak{p}^{\Sigma b-\Sigma a} = \mathfrak{p}^{l\frac{\Sigma b-\Sigma a}{l}} \sim 1.$$

Da die Zahl $r+1$ nicht durch l teilbar ist, wenn wir von dem Falle $l=3$ absehen, der für sich ohne weiteres klar liegt, so folgt aus den beiden Aequivalenzen (63.) und (64.) die im ersten Teile des Satzes 145 behauptete Aequivalenz.

Der zweite Teil des Satzes 145 folgt durch eingehendere Betrachtung der in § 112 entwickelten Congruenzeigenschaften (43.), (44.) der Lagrange'schen Wurzelzahl Λ.

Ein wesentlich verschiedener Beweis für den ersten Teil des Satzes 145 ergiebt sich unmittelbar aus einer gegen den Schluss des § 86 gemachten Bemerkung über den Ausdruck der Klassenanzahl des Körpers $k(\sqrt{-l})$ für den Fall $l\equiv 3$ nach 4.

Durch eine bemerkenswerte Modification des Jacobi'schen Verfahrens gelingt es, die Aussagen des Satzes 145 auch auf den Fall zu erweitern, dass die Primzahl p nicht von der Gestalt $p=ml+1$ ist. [*Eisenstein*[11], *Stickelberger*[1].]

§ 124.
Die Bestimmung des Vorzeichens der Gauss'schen Summe.

Es sei p eine ungerade rationale Primzahl, so können wir nach den Definitionen des § 111 und der in § 112 hinzugefügten Ausdehnung derselben auf den Fall $l = 2$ die Lagrange'sche Normalbasis und die Lagrange'sche Wurzelzahl für den quadratischen Körper $k\left(\sqrt{(-1)^{\frac{p-1}{2}}\,p}\right)$ aufstellen. Es werde $Z = e^{\frac{2i\pi}{p}}$ gesetzt, so besteht für diesen Körper die Lagrange'sche Normalbasis aus den zwei Zahlen

$$\lambda_0 = \sum_{(a)} Z^a, \quad \lambda_1 = \sum_{(b)} Z^b,$$

und die Lagrange'sche Wurzelzahl hat für ihn den Wert

$$\Lambda = \lambda_0 - \lambda_1 = \sum_{(a)} Z^a - \sum_{(b)} Z^b;$$

dabei durchlaufen a und b bez. die quadratischen Reste und Nichtreste nach p unter den Zahlen $1, 2, \ldots, p-1$.

Das am Schlusse des § 112 charakterisirte Problem der vollständigen Ermittelung von Λ, nachdem Λ^l gefunden ist, kommt in dem vorliegenden Falle des quadratischen Körpers auf die Frage nach einem gewissen Vorzeichen $\pm$ hinaus und wird durch folgenden Satz erledigt:

Satz 146. Die Lagrange'sche Wurzelzahl Λ des quadratischen Körpers mit der Primzahldiscriminante $(-1)^{\frac{p-1}{2}}\,p$ ist eine positiv reelle oder positiv rein imaginäre Zahl. [*Gauss*[2], *Kronecker*[4].]

Beweis. Das Quadrat der in Frage stehenden Lagrange'schen Wurzelzahl Λ besitzt, weil Λ eine Zahl des quadratischen Körpers und nach Satz 138

$$|\Lambda| = |\sqrt{p}|$$

ist, jedenfalls den Wert $(-1)^{\frac{p-1}{2}}\,p$; man hat also

$$\Lambda = \pm\sqrt{(-1)^{\frac{p-1}{2}}\,p}. \qquad (65.)$$

An die Stelle der in § 112 mit $\mathfrak{p}$, $\mathfrak{P}$ bezeichneten Ideale treten im vorliegenden Falle $l = 2$ bez. die Ideale (p) und $(1-Z)$; aus der Congruenz (43.) wird daher die Congruenz

$$A \equiv \frac{(-1)^{\frac{p+1}{2}}}{\frac{p-1}{2}!}(1-Z)^{\frac{p-1}{2}}, \quad (1-Z)^{\frac{p+1}{2}},$$

d. i.

$$(66.) \qquad A \equiv \frac{p-1}{2}! \quad (1-Z)^{\frac{p-1}{2}}, \quad (1-Z)^{\frac{p+1}{2}}.$$

Wir betrachten andererseits den Ausdruck

$$\Delta = (Z^{-1}-Z^{+1})(Z^{-2}-Z^{+2})\dots(Z^{-\frac{p-1}{2}}-Z^{+\frac{p-1}{2}}).$$

Da derselbe nur sein Vorzeichen ändert, wenn wir Z durch Z^R ersetzen wobei R eine Primitivzahl nach p bedeuten soll, und da das Ideal (Δ), mit dem Ideal $(1-Z)^{\frac{p-1}{2}}$ übereinstimmt, so ist notwendig

$$\Delta = \pm\sqrt{(-1)^{\frac{p-1}{2}}p}.$$

Um das Vorzeichen hier zu bestimmen, bedenken wir, dass

$$Z^{-h}-Z^{+h} = -2i\sin\frac{2h\pi}{p}, \quad \left(h=1,\ 2,\ \dots,\ \frac{p-1}{2}\right)$$

ist, und erhalten hieraus für Δ einen Wert von der Gestalt $(-i)^{\frac{p-1}{2}}P$, wo P eine positive Grösse darstellt. Hieraus folgt, wenn wir fortan unter $\sqrt{(-1)^{\frac{p-1}{2}}p}$ denjenigen Wert dieser Quadratwurzel verstehen, welcher positiv reell oder positiv rein imaginär ist,

$$(67.) \qquad \Delta = (-1)^{\frac{p^2-1}{8}}\sqrt{(-1)^{\frac{p-1}{2}}p}.$$

Endlich lehrt die Gleichung

$$\Delta = Z^{-1-2\dots-\frac{p-1}{2}}(1-Z^2)(1-Z^4)\dots(1-Z^{p-1}),$$

dass

$$\Delta \equiv 2.4.6\dots(p-1)(1-Z)^{\frac{p-1}{2}} \equiv 2^{\frac{p-1}{2}}\frac{p-1}{2}!(1-Z)^{\frac{p-1}{2}}, \quad (1-Z)^{\frac{p+1}{2}}$$

ist, und hieraus folgt nach (66.)

$$\Delta \equiv 2^{\frac{p-1}{2}}A, \quad (1-Z)^{\frac{p+1}{2}}.$$

Da

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}}, \quad (p)$$

wird, so ergiebt sich wegen (67.)

$$\varDelta \equiv \sqrt{(-1)^{\frac{p-1}{2}}\, p}, \quad (1-Z)^{\frac{p+1}{2}},$$

und folglich ist wegen (65.)

$$\varDelta = \sqrt{(-1)^{\frac{p-1}{2}}\, p},$$

womit der Satz 146 bewiesen ist.

Ueber specielle Abel'sche Körper von höherem als dem zweiten Grade ist bisher wenig veröffentlicht worden; erwähnt seien die *Eisenstein*'sche Abhandlung über cubische, aus der Kreisteilung entstehende Formen, welche als eine Einleitung in die Theorie der cubischen Abel'schen Körper aufzufassen ist [*Eisenstein* [10]], ferner die *Bachmann*'sche Arbeit über die aus zwei Quadratwurzeln zusammengesetzten complexen Zahlen [*Bachmann* [1]] und die *Weber*'schen Untersuchungen über Abel'sche cubische und biquadratische Zahlkörper [*Weber* [2, 4]].

Fünfter Teil.

Der Kummer'sche Zahlkörper.

Capitel XXVIII.

Die Zerlegung der Zahlen des Kreiskörpers im Kummer'schen Körper.

§ 125.

Die Definition des Kummer'schen Körpers.

Es bezeichne l eine ungerade rationale Primzahl und $k(\zeta)$ den durch $\zeta = e^{\frac{2i\pi}{l}}$ bestimmten Kreiskörper. Ist dann μ eine solche ganze Zahl in $k(\zeta)$, welche nicht zugleich die $l$te Potenz einer Zahl in $k(\zeta)$ wird, so erweist sich die Gleichung $l$ten Grades

$$x^l - \mu = 0$$

als irreducibel im Rationalitätsbereich $k(\zeta)$. Bedeutet $M = \sqrt[l]{\mu}$ eine irgendwie in bestimmter Weise ausgewählte Wurzel dieser Gleichung, so sind

$$\zeta M, \quad \zeta^2 M, \quad \ldots, \quad \zeta^{l-1} M$$

deren $l-1$ übrige Wurzeln. Den durch M und ζ bestimmten Körper $k(M, \zeta)$ nenne ich einen **Kummer'schen Körper.** Ein solcher Kummer'scher Körper $k(M, \zeta)$ ist vom Grade $l(l-1)$; er enthält den Kreiskörper $k(\zeta)$ als Unterkörper und ist in Bezug auf $k(\zeta)$ ein relativ Abel'scher Körper vom Relativgrade l. Durch die Operation der Vertauschung von M mit ζM in einer Zahl oder in einem Ideal dieses Kummer'schen Körpers geht man zu der relativ conjugirten Zahl bezüglich dem relativ

conjugirten Ideal über. Dieser Uebergang werde durch Vorsetzen des Substitutionszeichens S angedeutet.

Man beweist leicht die Thatsachen:

Satz 147. Der durch $M=\sqrt[l]{\mu}$ und ζ bestimmte Kummer'sche Körper ist im Bereiche der rationalen Zahlen dann und nur dann ein Galois'scher Körper, wenn unter den symbolischen Potenzen $\mu^{s-1}, \mu^{s-2}, \ldots, \mu^{s-l+1}$ eine die $l$te Potenz einer Zahl in $k(\zeta)$ wird. Dabei ist $s=(\zeta:\zeta^r)$, worin r eine Primitivzahl nach l bedeutet.

Der Kummer'sche Körper $k(M, \zeta)$ ist insbesondere dann und nur dann ein Abel'scher Körper, wenn μ^{s-r} die $l$te Potenz einer Zahl in $k(\zeta)$ wird.

Wenn der Kummer'sche Körper $k(M, \zeta)$ ein Galois'scher oder insbesondere ein Abel'scher Körper ist, so entsteht dieser Körper, wie man auf Grund der in § 38 entwickelten Begriffe ersieht, durch Zusammensetzung aus dem Kreiskörper $k(\zeta)$ und einem gewissen Körper $l$ten Grades.

§ 126.

Die Relativdiscriminante des Kummer'schen Körpers.

Unsere erste Aufgabe ist die Ermittelung der Relativdiscriminante von $k(M, \zeta)$ in Bezug auf $k(\zeta)$. Wir beweisen zunächst die folgende Thatsache:

Hülfssatz 23. Wenn ein Primideal $\mathfrak{p}$ des Kreiskörpers $k(\zeta)$ gleich der $l$ten Potenz eines Primideals $\mathfrak{P}$ des Kummer'schen Körpers $k(M, \zeta)$ wird und A eine ganze durch $\mathfrak{P}$, aber nicht durch $\mathfrak{P}^2$ teilbare Zahl in $k(M, \zeta)$ ist, so enthalten die Relativdiscriminante der Zahl A und die Relativdiscriminante des Kummer'schen Körpers $k(M, \zeta)$ in Bezug auf $k(\zeta)$ genau die gleiche Potenz von $\mathfrak{p}$ als Factor.

Beweis. Jede ganze Zahl des Kummer'schen Körpers $k(M, \zeta)$ ist offenbar in der Gestalt

$$(68.) \qquad \Omega=\frac{\alpha+\alpha_1 A+\alpha_2 A^2+\cdots+\alpha_{l-1} A^{l-1}}{\beta}$$

darstellbar, so dass $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{l-1}, \beta$ ganze Zahlen in $k(\zeta)$ sind. Ist dabei β durch $\mathfrak{p}$ teilbar, so folgt, dass auch der Zähler des rechter Hand stehenden Bruches congruent 0 nach $\mathfrak{p}$ sein muss. Wegen $A\equiv 0$ nach $\mathfrak{P}$ geht hieraus $\alpha\equiv 0$ nach $\mathfrak{P}$ und, da α in $k(\zeta)$ liegt, auch $\alpha\equiv 0$

nach $\mathfrak{p}$ hervor. Aus der letzten Congruenz ergiebt sich

$$\alpha_1 A + \alpha_2 A^2 + \cdots + \alpha_{l-1} A^{l-1} \equiv 0, \quad (\mathfrak{p}),$$

und da $A \not\equiv 0$, $A^2 \equiv 0$, $A^3 \equiv 0, \ldots, A^{l-1} \equiv 0$ nach $\mathfrak{P}^2$ ist, so folgt $\alpha_1 \equiv 0$ nach $\mathfrak{P}$ und daher auch nach $\mathfrak{p}$, also ist auch

$$\alpha_2 A^2 + \cdots + \alpha_{l-1} A^{l-1} \equiv 0, \quad (\mathfrak{p}).$$

Wegen $A^2 \not\equiv 0$, $A^3 \equiv 0, \ldots, A^{l-1} \equiv 0$ nach $\mathfrak{P}^3$ folgt $\alpha_2 \equiv 0$ nach $\mathfrak{P}$ und daher auch nach $\mathfrak{p}$. Fahren wir so fort, so erkennen wir, dass notwendig alle Coefficienten $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{l-1}$ durch $\mathfrak{p}$ teilbar sein müssen. Ist jetzt β' eine ganze Zahl in $k(\zeta)$, welche durch $\frac{\beta}{\mathfrak{p}}$ teilbar, aber nicht durch β teilbar ist, so werden die Zahlen $\alpha\beta', \alpha_1\beta', \ldots, \alpha_{l-1}\beta'$ sämtlich durch β teilbar. Wir setzen

$$\alpha' = \frac{\alpha\beta'}{\beta}, \quad \alpha'_1 = \frac{\alpha_1\beta'}{\beta}, \quad \ldots, \quad \alpha'_{l-1} = \frac{\alpha_{l-1}\beta'}{\beta}$$

und erhalten dann

$$(69.) \qquad \Omega = \frac{\alpha' + \alpha'_1 A + \alpha'_2 A^2 + \cdots + \alpha'_{l-1} A^{l-1}}{\beta'},$$

wo die im Nenner stehende Zahl β' jetzt einen Idealfactor $\mathfrak{p}$ weniger enthält als β. Wenden wir die eben auf (68.) angewandte Schlussweise nunmehr wiederum auf (69.) an u. s. f., so gelangen wir schliesslich zu dem Resultat, dass jede ganze Zahl Ω des Körpers $k(M, \zeta)$ in der Gestalt

$$(70.) \qquad \Omega = \frac{\bar{\alpha} + \bar{\alpha}_1 A + \bar{\alpha}_2 A^2 + \cdots + \bar{\alpha}_{l-1} A^{l-1}}{\bar{\beta}}$$

darstellbar ist derart, dass $\bar{\alpha}, \bar{\alpha}_1, \ldots, \bar{\alpha}_{l-1}, \bar{\beta}$ sämtlich ganze Zahlen in $k(\zeta)$ sind, und dass ausserdem $\bar{\beta}$ zu $\mathfrak{p}$ prim ausfällt. Wir denken uns nun die $l(l-1)$ Zahlen einer Basis des Kummer'schen Körpers $k(M, \zeta)$ gemäss (70.) ausgedrückt und bilden aus diesen Zahlen und den zu ihnen relativ conjugirten Zahlen die l-reihige Matrix; es wird dann ersichtlich, dass die Relativdiscriminante des Kummer'schen Körpers $k(M, \zeta)$ nach Multiplication mit gewissen zu $\mathfrak{p}$ primen ganzen Zahlen $\bar{\beta}$ des Körpers $k(\zeta)$ durch die Relativdiscriminante der Zahl A teilbar werden muss, und hiermit ist der Hülfssatz 23 bewiesen.

Satz 148. Es werde $\lambda = 1 - \zeta$ und $\mathfrak{l} = (\lambda)$ gesetzt. Geht ein

von $\mathfrak{l}$ verschiedenes Primideal $\mathfrak{p}$ des Kreiskörpers $k(\zeta)$ in der Zahl μ genau zur $e$ten Potenz auf, so enthält, wenn der Exponent e zu l prim ist, die Relativdiscriminante des durch $M = \sqrt[l]{\mu}$ und ζ bestimmten Kummer'schen Körpers in Bezug auf $k(\zeta)$ genau die Potenz $\mathfrak{p}^{l-1}$ von $\mathfrak{p}$ als Factor. Ist dagegen der Exponent e ein Vielfaches von l, so fällt diese Relativdiscriminante prim zu $\mathfrak{p}$ aus.

Was das Primideal $\mathfrak{l}$ betrifft, so können wir zunächst den Umstand ausschliessen, dass die Zahl μ durch $\mathfrak{l}$ teilbar ist und dabei $\mathfrak{l}$ genau in einer solchen Potenz enthält, deren Exponent ein Vielfaches von l ist; denn alsdann könnte die Zahl μ sofort durch eine zu $\mathfrak{l}$ prime Zahl μ^* ersetzt werden, so dass $k(\sqrt[l]{\mu^*}, \zeta)$ derselbe Körper wie $k(\sqrt[l]{\mu}, \zeta)$ ist. Unter Ausschluss des genannten Umstandes haben wir die zwei möglichen Fälle, dass μ genau eine Potenz von $\mathfrak{l}$ enthält, deren Exponent zu l prim ist, oder dass μ nicht durch l teilbar ist. Im ersteren Falle ist die Relativdiscriminante von $k(\sqrt[l]{\mu}, \zeta)$ in Bezug auf $k(\zeta)$ genau durch die Potenz $\mathfrak{l}^{l^2-1}$ von $\mathfrak{l}$ teilbar. Im zweiten Falle sei m der höchste Exponent $\leqq l$, für den es eine Zahl α in $k(\zeta)$ giebt, so dass $\mu \equiv \alpha^l$ nach $\mathfrak{l}^m$ ausfällt. Jene Relativdiscriminante ist dann im Falle $m = l$ zu $\mathfrak{l}$ prim; sie ist dagegen im Falle $m < l$ genau durch die Potenz $\mathfrak{l}^{(l-1)(l-m+1)}$ von $\mathfrak{l}$ teilbar.

Beweis. Gehen wir zunächst auf den ersten Teil des Satzes 148 ein. Es sei π eine durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbare ganze Zahl in $k(\zeta)$, und weiter sei ν eine durch $\frac{\pi}{\mathfrak{p}}$ teilbare, aber zu $\mathfrak{p}$ prime ganze Zahl in $k(\zeta)$.

Ist der Exponent e der in μ enthaltenen Potenz von $\mathfrak{p}$ kein Vielfaches von l, so können wir zwei ganze rationale positive Zahlen a und b bestimmen, so dass $1 = ae - bl$ ist. Dann ist $\mu^* = \frac{\mu^a \nu^{bl}}{\pi^{bl}}$ eine durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbare ganze Zahl in $k(\zeta)$, und es erweist sich, wenn $M^* = \sqrt[l]{\mu^*}$ gesetzt wird, $k(M^*, \zeta) = k(M, \zeta)$ und wenn wir den gemeinsamen Idealteiler von $\mathfrak{p}$ und M^* im Körper $k(M, \zeta)$ mit $\mathfrak{P}$ bezeichnen,

$$\mathfrak{P} = S\mathfrak{P}, \quad \mathfrak{p} = \mathfrak{P}^l.$$

Das Ideal $\mathfrak{P}$ ist also ein ambiges Primideal des Kummer'schen Körpers $k(M, \zeta)$ in Bezug auf den Unterkörper $k(\zeta)$; nach Satz 93 tritt dasselbe

daher in der Relativdiscriminante von $k(M, \zeta)$ in Bezug auf $k(\zeta)$ als Factor auf. Da ferner die Zahl M^* durch $\mathfrak{P}$, aber nicht durch $\mathfrak{P}^2$ teilbar ist, und da die Relativdiscriminante der Zahl M^* in Bezug auf $k(\zeta)$ den Wert $(-1)^{\frac{l-1}{2}} l^l \mu^{*l-1}$ hat, so ist nach Hülfssatz 23 das Ideal $\mathfrak{p}$ auch in der Relativdiscriminante des Körpers $k(M, \zeta)$ genau zur $(l-1)$ten Potenz enthalten.

Ist dagegen der Exponent e der in μ enthaltenen Potenz von $\mathfrak{p}$ ein Vielfaches von l, so ist $\mu^* = \frac{\mu \nu^e}{\pi^e}$ eine nicht durch $\mathfrak{p}$ teilbare ganze Zahl in $k(\zeta)$; da die Relativdiscriminante der Zahl $M^* = \sqrt[l]{\mu^*}$ in Bezug auf $k(\zeta)$ den Wert $(-1)^{\frac{l-1}{2}} l^l \mu^{*l-1}$ hat, so ist sie zu $\mathfrak{p}$ prim. Das Gleiche gilt mithin von der Relativdiscriminante des Körpers $k(M, \zeta)$ in Bezug auf $k(\zeta)$.

Jetzt betrachten wir die Verhältnisse in Betreff des Primfactors $\mathfrak{l}$. Im Falle, dass derselbe in μ zu einem solchen Exponenten e erhoben aufgeht, der kein Vielfaches von l ist, verfahren wir in entsprechender Weise, wie im ersten Teil dieses Beweises bei Behandlung des Primideales $\mathfrak{p}$ verfahren wurde, indem wir an die Stelle von μ eine Zahl μ^* bringen, die durch $\mathfrak{l}$, aber nicht durch $\mathfrak{l}^2$ teilbar ist. Da die Relativdiscriminante der Zahl $M^* = \sqrt[l]{\mu^*}$ den Wert $(-1)^{\frac{l-1}{2}} l^l \mu^{*l-1}$ hat, so ist, nach der Beschaffenheit von μ^*, dem Hülfssatze 23 zufolge die Relativdiscriminante des Körpers $k(M, \zeta)$ in Bezug auf $k(\zeta)$ genau durch $\mathfrak{l}^{l^2-1}$ teilbar.

An zweiter Stelle haben wir den Fall zu untersuchen, dass μ nicht durch $\mathfrak{l}$ teilbar ist. Der für diesen Fall in Satz 148 bezeichnete Exponent $m (\leqq l)$ sei zunächst $= l$; es gebe also eine ganze Zahl α in $k(\zeta)$ derart, dass $\mu \equiv \alpha^l$ nach $\mathfrak{l}^l$ ist; dabei wird dann $\frac{\mu - \alpha^l}{\lambda^l}$ eine ganze Zahl in $k(\zeta)$, und folglich besitzt die Gleichung $l$ten Grades in x

$$\frac{(\lambda x - \alpha)^l + \mu}{\lambda^l} = 0$$

lauter ganze Coefficienten. Da $x = \frac{\alpha - M}{\lambda}$, wo $M = \sqrt[l]{\mu}$ gesetzt ist, eine Wurzel dieser Gleichung ist, so erweist sich die Zahl $\Omega = \frac{\alpha - M}{\lambda}$ des Körpers $k(M, \zeta)$ als ganze Zahl. Die Relativdiscriminante dieser

Zahl Ω ist gleich $\varepsilon\mu^{l-1}$, wo ε eine Einheit bedeutet, und folglich ist auch die Relativdiscriminante des Körpers $k(M, \zeta)$ in Bezug auf $k(\zeta)$ zu $\mathfrak{l}$ prim.

Zweitens sei $m < l$, so dass also μ nicht einer $l$ten Potenz nach $\mathfrak{l}^l$ congruent gesetzt werden kann; wir setzen $\mu \equiv \alpha^l + a\lambda^m$ nach $\mathfrak{l}^{m+1}$, wo α eine ganze Zahl in $k(\zeta)$, ferner m der im Satze erklärte Exponent ist und a eine ganze rationale, nicht durch l teilbare Zahl bedeutet. Wir betrachten nun das Ideal

$$\mathfrak{A} = (\lambda,\ \alpha - M).$$

Die Zahl $\dfrac{\alpha - M}{\lambda}$ ist sicher keine ganze Zahl, da ihre Relativnorm in Bezug auf $k(\zeta)$, d. i. $\dfrac{\alpha^l - \mu}{\lambda^l}$, wegen $m < l$ eine gebrochene Zahl ist, also ist die Zahl $\alpha - M$ nicht durch $\mathfrak{l}$ teilbar; mithin ist das Ideal $\mathfrak{A}$ von $\mathfrak{l}$ verschieden. Andererseits ist $\mathfrak{A}$ auch nicht $= 1$, da die Relativnorm der Zahl $\alpha - M$ wegen

$$(71.) \qquad N_k(\alpha - M) = \alpha^l - \mu \equiv -a\lambda^m, \quad (\mathfrak{l}^{m+1})$$

durch $\mathfrak{l}^m$ teilbar ist. Da sich $S\mathfrak{A} = \mathfrak{A}$ erweist, so ist $\mathfrak{A}$ ein ambiges Ideal, und da dasselbe ein Factor von $\mathfrak{l}$ sein muss, so gehört unter den gegenwärtigen Umständen $\mathfrak{l}$ zur ersten von den drei in § 57 beim Beweise des Satzes 93 unterschiedenen Arten von Primidealen des Unterkörpers, d. h. wir haben $\mathfrak{l} = \mathfrak{L}^l$, wo $\mathfrak{L}$ ein Primideal und offenbar ersten Grades im Körper $k(M, \zeta)$ bedeutet. Aus der Congruenz (71.) ergiebt sich dann $\mathfrak{A} = \mathfrak{L}^m$.

Nunmehr bestimmen wir zwei ganze rationale positive Zahlen a und b, so dass $1 = am - bl$ wird, und setzen

$$\Omega = \frac{(\alpha - M)^a}{\lambda^b}.$$

Wegen $SM = \zeta M$ folgt

$$S\Omega = \frac{(\alpha - M + \lambda M)^a}{\lambda^b},$$

und wir schliessen aus diesem Ausdrucke, dass $\Omega - S\Omega$ genau durch die $(l - m + 1)$te Potenz von $\mathfrak{L}$ teilbar ist. Da von jeder Differenz aus irgend zwei zu Ω relativ conjugirten Zahlen das Gleiche gilt, so enthält die Relativdiscriminante der Zahl Ω in Bezug auf $k(\zeta)$ genau die

$(l-1)(l-m+1)$te Potenz des Ideals $\mathfrak{l}$. Hieraus folgt, indem Ω nur durch die erste Potenz von $\mathfrak{L}$ teilbar ist, nach Hülfssatz 23, dass auch die Relativdiscriminante des Körpers $k(M, \zeta)$ in Bezug auf $k(\zeta)$ genau durch die angegebene Potenz von $\mathfrak{l}$ teilbar sein muss.

Durch den eben bewiesenen Satz 148 ist die Relativdiscriminante des Kummer'schen Körpers $k(M, \zeta)$ in Bezug auf den Körper $k(\zeta)$ völlig bestimmt, und nach Satz 39 kann man aus dieser Relativdiscriminante sogleich auch die Discriminante des Kummer'schen Körpers $k(M, \zeta)$ finden.

§ 127.

Das Symbol $\left\{\frac{\mu}{\mathfrak{w}}\right\}$.

Für die weiteren Entwickelungen ist es nötig, das in § 113 eingeführte Symbol $\left\{\frac{\mu}{\mathfrak{w}}\right\}$ in folgender Weise zu verallgemeinern, so dass es auch in den Fällen eine Bedeutung hat, wo $\mathfrak{w}$ in μ aufgeht, und wo $\mathfrak{w} = \mathfrak{l}$ ist.

Es sei $\mathfrak{w}$ ein beliebiges Primideal in $k(\zeta)$ und μ eine beliebige ganze Zahl in $k(\zeta)$, welche nicht $l$te Potenz einer ganzen Zahl in $k(\zeta)$ ist. Wenn dann die Relativdiscriminante des durch $M = \sqrt[l]{\mu}$ und ζ bestimmten Kummer'schen Körpers durch $\mathfrak{w}$ teilbar ist, so habe das **Symbol** $\left\{\frac{\mu}{\mathfrak{w}}\right\}$ den Wert 0.

Ist dagegen die Relativdiscriminante dieses Körpers $k(M, \zeta)$ nicht durch $\mathfrak{w}$ teilbar, so kann man nach Satz 148 stets eine Zahl α in $k(\zeta)$ finden derart, dass $\mu^* = \alpha^l \mu$ eine ganze, nicht mehr durch $\mathfrak{w}$ teilbare Zahl in $k(\zeta)$ wird. Ist μ selbst zu $\mathfrak{w}$ prim, so erfüllt bereits $\alpha = 1$ diese Bedingung. Wir definiren dann, wenn $\mathfrak{w} \neq \mathfrak{l}$ ist, das fragliche **Symbol** durch die Formel

$$\left\{\frac{\mu}{\mathfrak{w}}\right\} = \left\{\frac{\mu^*}{\mathfrak{w}}\right\}.$$

Wenn aber $\mathfrak{w} = \mathfrak{l}$ ist, so kann, da die Relativdiscriminante von $k(M, \zeta)$ prim zu $\mathfrak{l}$ sein soll, nach dem Satze 148 die Zahl α überdies so gewählt werden, dass $\mu^* \equiv 1$ nach $\mathfrak{l}^l$ ausfällt. Ist dies geschehen, so gilt eine Congruenz von der Gestalt

$$\mu^* \equiv 1 + a\lambda^l, \quad (\mathfrak{l}^{l+1}),$$

wo a eine bestimmte Zahl aus der Reihe 0, 1, 2, ..., $l-1$ bedeutet. Ich definire dann das **Symbol** $\left\{\frac{\mu}{\mathfrak{l}}\right\}$ durch die Gleichung

$$\left\{\frac{\mu}{\mathfrak{l}}\right\}=\zeta^a.$$

Ist μ die $l$te Potenz einer ganzen Zahl in $k(\zeta)$ und $\mathfrak{w}$ ein beliebiges Primideal in $k(\zeta)$, so werde stets $\left\{\frac{\mu}{\mathfrak{w}}\right\}=1$ genommen.

Auf diese Weise ist der Wert des Symbols $\left\{\frac{\mu}{\mathfrak{w}}\right\}$ für jede ganze Zahl μ und für jedes Primideal $\mathfrak{w}$ in $k(\zeta)$ eindeutig festgelegt, und zwar wird dieser Wert entweder gleich 0 oder gleich einer bestimmten $l$ten Einheitswurzel.

Ist endlich $\mathfrak{a}$ ein beliebiges Ideal des Körpers $k(\zeta)$ und hat man $\mathfrak{a}=\mathfrak{p}\mathfrak{q}\ldots\mathfrak{w}$, wo $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{w}$ Primideale in $k(\zeta)$ sind, so möge, wenn μ eine beliebige ganze Zahl in $k(\zeta)$ ist, das **Symbol** $\left\{\frac{\mu}{\mathfrak{a}}\right\}$ durch die folgende Gleichung definirt werden:

$$\left\{\frac{\mu}{\mathfrak{a}}\right\}=\left\{\frac{\mu}{\mathfrak{p}}\right\}\left\{\frac{\mu}{\mathfrak{q}}\right\}\cdots\left\{\frac{\mu}{\mathfrak{w}}\right\}.$$

Sind $\mathfrak{a}$, $\mathfrak{b}$ beliebige Ideale in $k(\zeta)$, so gilt dann offenbar die Gleichung:

$$\left\{\frac{\mu}{\mathfrak{a}\mathfrak{b}}\right\}=\left\{\frac{\mu}{\mathfrak{a}}\right\}\left\{\frac{\mu}{\mathfrak{b}}\right\}.$$

§ 128.

Die Primideale des Kummer'schen Körpers.

Es sei μ eine ganze Zahl in $k(\zeta)$, aber $M=\sqrt[l]{\mu}$ keine Zahl dieses Körpers. Die Aufgabe, die Primideale des Kreiskörpers $k(\zeta)$ in Primideale des Kummer'schen Körpers $k(M,\zeta)$ zu zerlegen, wird durch folgenden Satz gelöst:

Satz 149. Ein beliebiges Primideal $\mathfrak{p}$ in $k(\zeta)$ ist in dem durch $M=\sqrt[l]{\mu}$ und ζ bestimmten Kummer'schen Körper $k(M,\zeta)$ entweder gleich der $l$ten Potenz eines Primideals oder zerlegbar in l von einander verschiedene Primideale oder selbst Primideal, je nachdem $\left\{\frac{\mu}{\mathfrak{p}}\right\}=0$ oder $=1$ oder gleich einer von 1 verschiedenen $l$ten Einheitswurzel ausfällt.

Beweis. Der erste Teil dieses Satzes bezieht sich auf die in der Relativdiscriminante des Kummer'schen Körpers $k(M, \zeta)$ aufgehenden Primideale; dieselben sind nach Satz 93 ambig. Hieraus oder aus dem Beweise des Satzes 148 ergiebt sich für diese Primideale die Richtigkeit der Behauptung.

Wenn $\mathfrak{p}$ ein nicht in der Relativdiscriminante des Körpers $k(M, \zeta)$ aufgehendes Primideal ist, so möge μ^* eine durch $\mathfrak{p}$ nicht teilbare ganze Zahl von der Art sein, dass der Quotient $\frac{\mu^*}{\mu}$ gleich der $l$ten Potenz einer Zahl in $k(\zeta)$ ist. Der Körper $k(M, \zeta)$ wird dann auch durch $M^* = \sqrt[l]{\mu^*}$ und ζ festgelegt.

Wir untersuchen zunächst den Fall, dass $\mathfrak{p} \neq \mathfrak{l}$ ist. Wenn dann $\left\{\frac{\mu^*}{\mathfrak{p}}\right\} = 1$ ausfällt, so ist nach Satz 139 die Zahl μ^* ein $l$ter Potenzrest nach $\mathfrak{p}$. Wir bestimmen, was offenbar möglich ist, eine ganze Zahl α in $k(\zeta)$ derart, dass

$$\mu^* \equiv \alpha^l, \quad (\mathfrak{p}) \qquad \text{und} \qquad \mu^* \not\equiv \alpha^l, \quad (\mathfrak{p}^2)$$

wird; alsdann bilden wir die relativ conjugirten Ideale

$$\begin{aligned} \mathfrak{P} &= (\mathfrak{p},\ M^* - \alpha), \\ S\mathfrak{P} &= (\mathfrak{p},\ \zeta M^* - \alpha), \\ &\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ S^{l-1}\mathfrak{P} &= (\mathfrak{p},\ \zeta^{l-1} M^* - \alpha) \end{aligned}$$

und erhalten leicht

$$\mathfrak{p} = \mathfrak{P} . S\mathfrak{P} \ldots S^{l-1}\mathfrak{P}.$$

Wegen

$$(\mathfrak{P},\ S\mathfrak{P}) = (\mathfrak{p},\ M^* - \alpha,\ \zeta M^* - \alpha) = 1$$

ist $S\mathfrak{P}$ von $\mathfrak{P}$, und folglich sind alle l Primfactoren $\mathfrak{P}, S\mathfrak{P}, \ldots, S^{l-1}\mathfrak{P}$ des Ideals $\mathfrak{p}$ unter einander verschieden. Das Primideal $\mathfrak{p}$ in $k(\zeta)$ gehört also zu der zweiten der drei im Beweise zu Satz 93 aufgezählten Arten von Primidealen des Unterkörpers: es zerfällt in $k(M, \zeta)$ in l von einander verschiedene Primideale. Umgekehrt, wenn ein Primideal $\mathfrak{p}$ des Körpers $k(\zeta)$, wo jetzt $\mathfrak{p}$ auch $= \mathfrak{l}$ sein kann, in l von einander verschiedene Primideale $\mathfrak{P}, S\mathfrak{P}, \ldots, S^{l-1}\mathfrak{P}$ des Körpers $k(M, \zeta)$ zerfällt, so wird, wenn p die durch $\mathfrak{p}$ teilbare rationale Primzahl $N(\mathfrak{P}) = p^f$ und die Norm von $\mathfrak{P}$ ist,

$$N(\mathfrak{p}) = N(\mathfrak{P}) N(S\mathfrak{P}) \ldots N(S^{l-1}\mathfrak{P}) = p^{lf},$$

und mithin ist die Norm von $\mathfrak{p}$, im Körper $k(\zeta)$ genommen, $n(\mathfrak{p})$, ebenfalls gleich p^f. Die Gleichheit der Normen $N(\mathfrak{P})$ und $n(\mathfrak{p})$ lässt, wie in § 57, die Thatsache erkennen, dass eine jede ganze Zahl des Körpers $k(M, \zeta)$ einer ganzen Zahl des Körpers $k(\zeta)$ nach $\mathfrak{P}$ congruent gesetzt werden kann; setzen wir insbesondere $M^* \equiv \alpha$ nach $\mathfrak{P}$, wo α in $k(\zeta)$ liegen soll, so folgt $M^{*l} = \mu^* \equiv \alpha^l$ nach $\mathfrak{P}$, und da $\mu^* - \alpha^l$ eine Zahl in $k(\zeta)$ ist, so muss $\mu^* \equiv \alpha^l$ auch nach $\mathfrak{p}$ sein, d. h. es gilt $\left\{\frac{\mu^*}{\mathfrak{p}}\right\} = \left\{\frac{\mu}{\mathfrak{p}}\right\} = 1$. Damit ist zugleich für ein von $\mathfrak{l}$ verschiedenes Primideal $\mathfrak{p}$ der letzte Teil des Satzes 149 vollständig bewiesen.

Was endlich das Primideal $\mathfrak{l}$ anbetrifft, so gilt, falls die Relativdiscriminante des Körpers $k(M, \zeta)$ in Bezug auf $k(\zeta)$ durch $\mathfrak{l}$ nicht teilbar ist, für die Zahl μ^* dem Satze 148 gemäss eine Congruenz von der Gestalt

$$\mu^* \equiv \alpha^l + a\lambda^l, \quad (\mathfrak{l}^{l+1}),$$

wo a eine ganze rationale Zahl bedeutet. Soll nun $\left\{\frac{\mu}{\mathfrak{l}}\right\} = 1$, d. h. a durch l teilbar sein, so folgt daraus eine Congruenz von der Gestalt

$$\mu^* \equiv \alpha^l + a^* \lambda^{l+1}, \quad (\mathfrak{l}^{l+2}),$$

wo a^* wiederum eine ganze rationale Zahl bedeutet. Ist hierin a^* nicht durch l teilbar, so setzen wir $\mu^{**} = \mu^*$; ist dagegen a^* durch l teilbar, so setzen wir $\mu^{**} = (1+\lambda)^l \mu^* = (1-\lambda^2)^l \mu^*$, dann folgt

$$\mu^{**} \equiv \alpha^l + \lambda^{l+1} \alpha^l, \quad (\mathfrak{l}^{l+2}).$$

Demnach genügt die Zahl μ^{**} stets einer Congruenz

$$\mu^{**} \equiv \alpha^l + a^{**} \lambda^{l+1}, \quad (\mathfrak{l}^{l+2}),$$

wo nun a^{**} eine ganze rationale, nicht durch l teilbare Zahl bedeutet, und hieraus folgt, wenn $M^{**} = \sqrt[l]{\mu^{**}}$ und

$$\mathfrak{L} = \left(\lambda, \ \frac{\alpha - M^{**}}{\lambda}\right)$$

gesetzt wird, für $\mathfrak{l}$ die Zerlegung

$$\mathfrak{l} = \mathfrak{L} . S\mathfrak{L} \ldots S^{l-1}\mathfrak{L}.$$

Wegen

$$\left(\lambda, \ \frac{\alpha - M^{**}}{\lambda}, \ \frac{\alpha - \zeta M^{**}}{\lambda}\right) = 1$$

ist $S\mathfrak{L}$ von $\mathfrak{L}$ verschieden, und daher sind auch alle l Primideale $\mathfrak{L}$, $S\mathfrak{L}, \ldots, S^{l-1}\mathfrak{L}$ unter einander verschieden.

Umgekehrt, wenn $\mathfrak{l}$ eine Zerlegung dieser Art im Kummer'schen Körper $k(M, \zeta)$ gestattet, so stimmen nach einer oben gemachten und, wie dort erwähnt, auch für $\mathfrak{p} = \mathfrak{l}$ zutreffenden Bemerkung die Normen von $\mathfrak{L}$ in $k(M, \zeta)$ und von $\mathfrak{l}$ in $k(\zeta)$ überein, und es muss daher jede ganze Zahl des Körpers $k(M, \zeta)$ einer ganzen Zahl des Körpers $k(\zeta)$ nach $\mathfrak{L}$ congruent sein. Da $\mathfrak{l}$ alsdann nach Satz 93 gewiss nicht in der Relativdiscriminante des Körpers $k(M, \zeta)$ in Bezug auf $k(\zeta)$ enthalten ist, so können wir nach Satz 148 $\mu^* \equiv \alpha^l$ nach $\mathfrak{l}^l$ setzen, und demgemäss ist $\dfrac{\alpha - M^*}{\lambda}$ eine ganze Zahl. Da $\mathfrak{L}$ ein Primideal ersten Grades in $k(M, \zeta)$ wird, so können wir diese ganze Zahl congruent a nach $\mathfrak{L}$ setzen, so dass a eine ganze rationale Zahl bedeutet; dann folgt, wenn N_k als Bezeichnung der Relativnorm in Bezug auf $k(\zeta)$ dient, die Congruenz

$$N_k\left(\frac{\alpha - M^*}{\lambda} - a\right) \equiv 0, \quad (\mathfrak{l}),$$

d. h.

$$(\alpha - a\lambda)^l - \mu^* \equiv 0, \quad (\mathfrak{l}^{l+1});$$

es ist mithin $\left\{\dfrac{\mu^*}{\mathfrak{l}}\right\} = \left\{\dfrac{\mu}{\mathfrak{l}}\right\} = 1$. Diese Thatsachen beweisen auch für das Primideal $\mathfrak{l}$ den letzten Teil des Satzes 149.

Durch den Satz 149 haben wir ein einfaches Mittel erlangt, um die im Beweise des Satzes 93 aufgezählten drei Arten von Primidealen eines Körpers in Hinsicht auf einen relativ-cyklischen Oberkörper von einem Primzahlrelativgrade für den vorliegenden Fall der Körper $k(M, \zeta)$ und $k(\zeta)$ zu unterscheiden.

Capitel XXIX.

Die Normenreste und Normennichtreste des Kummer'schen Körpers.

§ 129.

Die Definition der Normenreste und Normennichtreste.

Es sei, wie in § 125, μ eine Zahl des Kreiskörpers $k(\zeta)$, für welche $M = \sqrt[l]{\mu}$ nicht in $k(\zeta)$ liegt, und es bedeute $k(M, \zeta)$ den durch M

und ζ bestimmten Kummer'schen Körper; für eine Zahl A in $k(M, \zeta)$ werde die Relativnorm in Bezug auf $k(\zeta)$ mit $N_k(A)$ bezeichnet. Es sei $\mathfrak{w}$ ein beliebiges Primideal des Kreiskörpers $k(\zeta)$ und ν eine beliebige ganze Zahl in $k(\zeta)$. Wenn dann ν nach $\mathfrak{w}$ der Relativnorm einer ganzen Zahl des Körpers $k(M, \zeta)$ congruent ist, und wenn ausserdem auch für jede höhere Potenz von $\mathfrak{w}$ stets eine solche ganze Zahl A im Körper $k(M, \zeta)$ gefunden werden kann, dass $\nu \equiv N_k(A)$ nach jener Potenz von $\mathfrak{w}$ ausfällt, so nenne ich ν einen **Normenrest des Kummer'schen Körpers $k(M, \zeta)$ nach $\mathfrak{w}$**. In jedem anderen Falle nenne ich ν einen **Normennichtrest des Kummer'schen Körpers $k(M, \zeta)$ nach $\mathfrak{w}$**.

§ 130.

Der Satz von der Anzahl der Normenreste. Die Verzweigungsideale.

Es gilt der folgende wichtige Satz:

Satz 150. Wenn $\mathfrak{w}$ ein Primideal des Kreiskörpers $k(\zeta)$ ist, das nicht in der Relativdiscriminante des Kummer'schen Körpers $k(M, \zeta)$ aufgeht, so ist jede zu $\mathfrak{w}$ prime Zahl in $k(\zeta)$ Normenrest des Kummer'schen Körpers $k(M, \zeta)$ nach $\mathfrak{w}$.

Wenn dagegen $\mathfrak{w}$ ein Primideal des Kreiskörpers $k(\zeta)$ ist, das in der Relativdiscriminante des Kummer'schen Körpers $k(M, \zeta)$ aufgeht, und e im Falle $\mathfrak{w} \neq \mathfrak{l}$ ein beliebiger positiver Exponent, im Falle $\mathfrak{w} = \mathfrak{l}$ ein beliebiger Exponent $> l$ bedeutet, so sind von allen vorhandenen, zu $\mathfrak{w}$ primen und nach $\mathfrak{w}^e$ einander incongruenten Zahlen in $k(\zeta)$ genau der $l$te Teil Normenreste nach $\mathfrak{w}$.

Beweis. Es sei zunächst $\mathfrak{w}$ ein in der Relativdiscriminante des Körpers $k(M, \zeta)$ nicht aufgehendes und von $\mathfrak{l}$ verschiedenes Primideal des Kreiskörpers $k(\zeta)$; dann sind zwei Fälle zu unterscheiden, je nachdem $\mathfrak{w}$ in $k(M, \zeta)$ zerlegbar ist oder nicht. Im ersteren Falle sei $\mathfrak{W}$ ein in $\mathfrak{w}$ aufgehendes Primideal des Kummer'schen Körpers $k(M, \zeta)$. Im Hinblick auf den Beweis zu Satz 148 können wir, ohne dadurch eine Beschränkung einzuführen, annehmen, es sei μ und mithin auch die Relativdiscriminante der Zahl $M = \sqrt[l]{\mu}$ in Bezug auf $k(\zeta)$ nicht durch $\mathfrak{W}$ teilbar; es giebt dann gewiss im Körper $k(M, \zeta)$ ein System von l ganzen Zahlen $A_1, \ldots, A_l$, für welche die l Congruenzen

$$\left.\begin{array}{ll} A_1+A_2M+\cdots+A_lM^{l-1} & \equiv \nu, \\ A_1+A_2\zeta M+\cdots+A_l(\zeta M)^{l-1} & \equiv 1, \\ A_1+A_2\zeta^2M+\cdots+A_l(\zeta^2M)^{l-1} & \equiv 1, \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot & \\ A_1+A_2\zeta^{l-1}M+\cdots+A_l(\zeta^{l-1}M)^{l-1} & \equiv 1, \end{array}\right\} (\mathfrak{W})$$

erfüllt sind. Nun ist offenbar jede ganze Zahl des Körpers $k(M, \zeta)$ nach $\mathfrak{W}$ einer ganzen Zahl in $k(\zeta)$ congruent; setzen wir

$$A_1 \equiv \alpha_1, \quad A_2 \equiv \alpha_2, \quad \ldots, \quad A_l \equiv \alpha_l, \quad (\mathfrak{W}),$$

so dass $\alpha_1, \alpha_2, \ldots, \alpha_l$ ganze Zahlen in $k(\zeta)$ sind, und

$$A = \alpha_1+\alpha_2M+\cdots+\alpha_lM^{l-1},$$

so ergiebt sich daher

$$\nu \equiv A, \quad 1 \equiv SA, \quad \ldots, \quad 1 \equiv S^{l-1}A, \quad (\mathfrak{W}),$$

und durch Multiplication folgt $\nu \equiv N_k(A)$ nach $\mathfrak{W}$ und daher auch nach $\mathfrak{w}$. Damit ist unter der gegenwärtigen Annahme über das Primideal $\mathfrak{w}$ der erste Teil des Satzes für den Fall $e=1$ bewiesen. Um zu den Fällen $e>1$ überzugehen, nehmen wir an, es sei $\nu \equiv\!\!|\!\!\equiv N_k(A)$ nach $\mathfrak{w}^2$, und setzen dann

$$\frac{\nu}{N_k(A)} \equiv 1+\omega, \quad (\mathfrak{w}^2),$$

so dass dabei ω eine ganze, durch $\mathfrak{w}$, aber nicht durch $\mathfrak{w}^2$ teilbare Zahl in $k(\zeta)$ bedeutet. Die ganze Zahl $B = A(1+l^*\omega)$, wobei l^* eine ganze rationale, der Congruenz $ll^* \equiv 1$ nach $\mathfrak{w}$ genügende Zahl sein soll, erfüllt dann die Bedingung $\nu \equiv N_k(B)$ nach $\mathfrak{w}^2$. Durch die gehörige Fortsetzung des hier eingeschlagenen Verfahrens gelangen wir schliesslich zu einer ganzen Zahl in $k(M, \zeta)$, deren Relativnorm in Bezug auf $k(\zeta)$ der Zahl ν nach einer beliebig hohen Potenz $\mathfrak{w}^e$ congruent ist.

Es sei andererseits $\mathfrak{w}$ im Körper $k(M, \zeta)$ nicht weiter zerlegbar; wir können es wiederum einrichten, dass μ nicht durch $\mathfrak{w}$ teilbar sei, und es ist dann nach Satz 149 μ jedenfalls kein $l$ter Potenzrest nach $\mathfrak{w}$. Nach den Folgerungen aus Satz 139 giebt es in $k(\zeta)$ genau $r = \dfrac{n(\mathfrak{w})-1}{l}$ zu $\mathfrak{w}$ prime $l$te Potenzreste nach $\mathfrak{w}$; sind diese nach $\mathfrak{w}$ durch $\varrho_1, \ldots, \varrho_r$

vertreten, so fallen die $n(\mathfrak{w})-1$ Zahlen

$$\varrho_i \mu^g \qquad \begin{pmatrix} i = 1, 2, \ldots, r, \\ g = 0, 1, 2, \ldots, l-1 \end{pmatrix}$$

sämtlich nach $\mathfrak{w}$ unter einander incongruent aus, da μ nicht $l$ter Potenzrest nach $\mathfrak{w}$ ist, und es ist also jede zu $\mathfrak{w}$ prime Zahl in $k(\zeta)$ einer dieser Zahlen nach $\mathfrak{w}$ congruent. Setzen wir $\varrho_1 \equiv \alpha_1^l, \ldots, \varrho_r \equiv \alpha_r^l$ nach $\mathfrak{w}$, so dass $\alpha_1, \ldots, \alpha_r$ ebenfalls Zahlen in $k(\zeta)$ sind, so folgt

$$\varrho_i \mu^g \equiv N_k(\alpha_i M^g), \quad (\mathfrak{w})$$

und es ist also jede zu $\mathfrak{w}$ prime Zahl in $k(\zeta)$ der Norm einer geeigneten Zahl in $k(M, \zeta)$ nach $\mathfrak{w}$ congruent; hieraus schliesst man weiter, ähnlich wie im vorigen Falle, dass zu jeder zu $\mathfrak{w}$ primen ganzen Zahl ν in $k(\zeta)$ auch in Bezug auf eine beliebig hohe Potenz $\mathfrak{w}^e$ von $\mathfrak{w}$ stets eine ganze Zahl des Körpers $k(M, \zeta)$ gefunden werden kann, deren Relativnorm nach $\mathfrak{w}^e$ der Zahl ν congruent ist.

Wir wollen nun den ersten Teil des Satzes 150 auch für den Fall $\mathfrak{w} = \mathfrak{l}$ beweisen, dabei können wir μ zu $\mathfrak{l}$ prim annehmen; wir bezeichnen mit λ^m die höchste in $\mu^{l-1}-1$ enthaltene Potenz von λ, wobei jedenfalls $m \geqq 1$ sein wird, und setzen

$$\mu^{l-1} \equiv 1 + a\lambda^m, \quad (\mathfrak{l}^{m+1}),$$

wo a eine ganze rationale, zu l prime Zahl bedeuten soll. Ist dann a^* eine ganze rationale Zahl mit der Congruenzeigenschaft $aa^* \equiv -1$ nach l, und setzen wir $\mu^* = \mu^{a^*(l-1)}$, so wird

$$(72.) \qquad \mu^* \equiv 1 - \lambda^m, \quad (\mathfrak{l}^{m+1}).$$

Andererseits gelten die Congruenzen

$$(73.) \qquad \left\{ \begin{aligned} (1-\lambda^{g+1})^l &\equiv 1 + \lambda^{l+g} \\ (1-\lambda^{g+1})^{hl} &\equiv 1 + h\lambda^{l+g} \end{aligned} \right\}, \quad (\mathfrak{l}^{l+g+1}),$$

wo g eine jede positive ganze rationale Zahl und h eine jede positive ganze rationale zu l prime Zahl sein kann. Da die Relativdiscriminante des Körpers $k(M, \zeta)$ in Bezug auf $k(\zeta)$ im gegenwärtig zu untersuchenden Falle den Factor $\mathfrak{l}$ nicht enthalten soll, so ist nach Satz 148 notwendig $m \geqq l$.

Es sei zunächst $m = l$. Man entnimmt dann leicht aus den Congruenzen (72.) und (73.), dass zu jeder beliebigen positiven ganzen rationalen Zahl g stets eine ganze Zahl α_g in $k(\zeta)$ gefunden werden kann derart,

dass die Congruenz

$$\mu^*\alpha_g^l \equiv 1-\lambda^l+\lambda^{l+g}, \quad (\mathfrak{l}^{l+g+1})$$

erfüllt wird. Setzen wir nun $M^* = \sqrt[l]{\mu^*}$ und ferner allgemein für jeden Wert von g:

$$\Omega_g = \frac{1-\alpha_g M^*}{\lambda},$$

so wird jedesmal Ω_g eine ganze Zahl in $k(M,\zeta)$ und

$$N_k(\Omega_g) \equiv 1-\lambda^g, \quad (\mathfrak{l}^{g+1}).$$

Hieraus folgt unmittelbar, dass jede ganze Zahl ν in $k(\zeta)$, die der Congruenz $\nu\equiv 1$ nach $\mathfrak{l}$ genügt, Normenrest des Körpers $k(M,\zeta)$ nach $\mathfrak{l}$ ist. Die Beschränkung, die hier in Annahme $\nu\equiv 1$ nach $\mathfrak{l}$ liegt, wird leicht aufgehoben. Ist nämlich ν eine beliebige zu $\mathfrak{l}$ prime Zahl, und wird sie nach $\mathfrak{l}$ der ganzen rationalen Zahl a congruent, so setzen wir $\nu^* = a^{*l}\nu$, wo a^* eine ganze rationale Zahl mit der Congruenzeigenschaft $aa^*\equiv 1$ nach $\mathfrak{l}$ bedeute; dann wird offenbar $\nu^*\equiv 1$ nach $\mathfrak{l}$, und andererseits werden ν und ν^* gleichzeitig Normenrest oder Normennichtrest des Körpers $k(M,\zeta)$ nach $\mathfrak{l}$ sein.

Es sei zweitens in Formel (72.) $m>l$ und mithin $\left\{\frac{\mu}{\mathfrak{l}}\right\}=1$; dann können wir, wenn g eine beliebige positive ganze rationale Zahl ist, stets zwei ganze Zahlen α_g und α_{g+1} in $k(\zeta)$ construiren derart, dass

$$(74.)\quad \begin{cases} \mu^*\alpha_g^l \equiv 1+\lambda^{l+1}+\lambda^{l+g+1}, & (\mathfrak{l}^{l+g+2}), \\ \mu^*\alpha_{g+1}^l \equiv 1+\lambda^{l+1}+\lambda^{l+g+2}, & (\mathfrak{l}^{l+g+3}) \end{cases}$$

wird. Wir setzen gemäss dem Satze 149 $\mathfrak{l}=\mathfrak{L}\mathfrak{L}'\ldots\mathfrak{L}^{(l-1)}$, wo $\mathfrak{L}, \mathfrak{L}', \ldots$ $\ldots, \mathfrak{L}^{(l-1)}$ von einander verschiedene Primideale des Körpers $k(M,\zeta)$ bedeuten. Die beiden Zahlen

$$A_g = \frac{1-\alpha_g M^*}{\lambda}, \quad A_{g+1} = \frac{1-\alpha_{g+1} M^*}{\lambda},$$

$M^* = \sqrt[l]{\mu^*}$ gesetzt, sind ganze Zahlen, und da $N_k(A_g)\equiv -\lambda$ nach $\mathfrak{l}^2$ wird, so enthält A_g eines der in $\mathfrak{l}$ aufgehenden Primideale, es sei dies etwa das Primideal $\mathfrak{L}$, zur ersten Potenz und die anderen in $\mathfrak{l}$ aufgehenden Primideale gar nicht. Aus den Formeln (74.) folgt

$$\alpha_g^l \equiv \alpha_{g+1}^l, \quad (\mathfrak{l}^{l+2}),$$

und wir können nun voraussetzen, dass α_{g+1} in der Reihe der Zahlen $\alpha_{g+1}, \zeta\alpha_{g+1}, \ldots, \zeta^{l-1}\alpha_{g+1}$ in solcher Weise gewählt sei, dass $\alpha_g \equiv \alpha_{g+1}$ nach $\mathfrak{l}^2$ und also $A_g \equiv A_{g+1}$ nach $\mathfrak{l}$ ausfällt. Wegen der letzteren Congruenz ist auch die Zahl A_{g+1} durch $\mathfrak{L}$, aber durch keines der Primideale $\mathfrak{L}', \ldots, \mathfrak{L}^{(l-1)}$ teilbar, und da auch $N_k(A_{g+1}) \equiv -\lambda$ nach $\mathfrak{l}^2$ ist, so ist A_{g+1} ebenfalls nur durch die erste Potenz von $\mathfrak{L}$ teilbar. Wir können mit Rücksicht auf das eben Bewiesene die gebrochene Zahl $\dfrac{A_g}{A_{g+1}}$ in die Form eines Bruches schreiben, dessen Zähler und Nenner zu $\mathfrak{l}$ prim sind. Setzen wir $\dfrac{A_g}{A_{g+1}} \equiv \Omega_g$ nach $\mathfrak{l}^{g+1}$ in solcher Weise, dass Ω_g eine ganze Zahl in $k(M,\zeta)$ ist, so wird

$$N_k(\Omega_g) \equiv \frac{N_k(A_g)}{N_k(A_{g+1})} \equiv 1 + \lambda^g, \quad (\mathfrak{l}^{g+1}).$$

Da eine solche Formel für jeden positiven Exponenten g möglich ist, so zeigt sich wie vorhin, dass jede zu $\mathfrak{l}$ prime Zahl Normenrest des Körpers $k(M,\zeta)$ ist.

Wir gehen jetzt zum Beweise der zweiten Hälfte von Satz 150 über. Es sei zunächst $\mathfrak{w}$ ein von $\mathfrak{l}$ verschiedenes, in der Relativdiscriminante des Körpers $k(M,\zeta)$ in Bezug auf $k(\zeta)$ aufgehendes Primideal des Körpers $k(\zeta)$; wir haben dann nach Satz 149 $\mathfrak{w} = \mathfrak{W}^l$, wo $\mathfrak{W}$ ein Primideal in $k(M,\zeta)$ ist. Jede ganze Zahl des Körpers $k(M,\zeta)$ muss dann, wie schon mehrfach erwähnt wurde, einer ganzen Zahl in $k(\zeta)$ nach $\mathfrak{W}$ congruent sein. Soll nun eine gegebene, zu $\mathfrak{w}$ prime ganze Zahl ν in $k(\zeta)$ nach $\mathfrak{w}$ congruent der Relativnorm $N_k(A)$ einer ganzen Zahl A in $k(M,\zeta)$ sein, und setzen wir $A \equiv \alpha$ nach $\mathfrak{W}$, so folgt notwendig $\nu \equiv \alpha^l$ nach $\mathfrak{W}$, und daher auch nach $\mathfrak{w}$, d. h. ν ist $l$ter Potenzrest nach $\mathfrak{w}$. Umgekehrt, wenn eine Zahl ν in $k(\zeta)$ ein $l$ter Potenzrest nach $\mathfrak{w}$ ist, so ist ν offenbar auch congruent einer Relativnorm $N_k(A)$ nach $\mathfrak{w}$. Wir entnehmen hieraus, dass die $l$ten Potenzreste nach $\mathfrak{w}$ auch zugleich die sämtlichen Normenreste des Körpers $k(M,\zeta)$ nach $\mathfrak{w}$ liefern.

Es bleibt endlich die Behandlung des Falles übrig, dass $\mathfrak{w} = \mathfrak{l}$ ist und $\mathfrak{l}$ in der Relativdiscriminante des Körpers $k(M,\zeta)$ aufgeht. Wir haben in diesem Falle $\mathfrak{l} = \mathfrak{L}^l$, wo $\mathfrak{L}$ ein Primideal in $k(M,\zeta)$ ist, und können es im Hinblick auf Satz 148 stets einrichten, dass die Zahl μ entweder der Congruenz

$$\mu \equiv \lambda, \qquad (\mathfrak{l}^2)$$

oder einer der folgenden Congruenzen genügt:

$$\mu \equiv 1+\lambda^m, \quad (\mathfrak{l}^{m+1}),$$

wo m einen der Werte 1, 2, ..., $l-1$ bedeutet. Wir wollen alsdann untersuchen, welche Zahlen in $k(\zeta)$ es in diesen zwei Fällen giebt, die congruent der Relativnorm einer Zahl in $k(M,\zeta)$ nach $\mathfrak{l}^{l+1}$ bez. $\mathfrak{l}^l$ sind, und entnehmen hieraus leicht die Anzahl der nach jeder höheren Potenz von $\mathfrak{l}$ einander incongruenten Normenreste.

Im Falle $\mu \equiv \lambda$ nach $\mathfrak{l}^2$ ist M durch $\mathfrak{L}$, aber nicht durch $\mathfrak{L}^2$ teilbar, und es gelten die Congruenzen

$$(75.)\quad \begin{cases} N_k(1+M) \equiv 1+\lambda, & (\mathfrak{l}^2), \\ \text{d. i.}\quad N_k(1+M) \equiv 1+\lambda \quad +\lambda^2\varrho_1, & (\mathfrak{l}^{l+1}), \\ N_k(1+M^2) \equiv 1+\lambda^2, & (\mathfrak{l}^3), \\ \text{d. i.}\quad N_k(1+M^2) \equiv 1+\lambda^2 \quad +\lambda^3\varrho_2, & (\mathfrak{l}^{l+1}), \\ \cdots\cdots\cdots & \\ N_k(1+M^{l-1}) \equiv 1+\lambda^{l-1}, & (\mathfrak{l}^l), \\ \text{d. i.}\quad N_k(1+M^{l-1}) \equiv 1+\lambda^{l-1}+\lambda^l\varrho_{l-1}, & (\mathfrak{l}^{l+1}), \end{cases}$$

wo $\varrho_1, \varrho_2, \ldots, \varrho_{l-1}$ gewisse ganze Zahlen in $k(\zeta)$ bedeuten. Endlich ist

$$(76.)\qquad N_k(1+\lambda^t M^g) \equiv 1, \quad (\mathfrak{l}^{l+1})$$

für $t=1, 2, 3, \ldots$; $g=0, 1, 2, \ldots, l-1$. Nun genügt offenbar jede zu $\mathfrak{L}$ prime ganze Zahl A des Körpers $k(M,\zeta)$ einer Congruenz von der Gestalt

$$\begin{aligned} A \equiv a(1+M)^{a_1} & (1+M^2)^{a_2} \ldots (1+M^{l-1})^{a_{l-1}} \\ & (1+\lambda\, M)^{a'_1}(1+\lambda\, M^2)^{a'_2}\ldots(1+\lambda\, M^{l-1})^{a'_{l-1}} \\ & \cdots\cdots\cdots \\ & (1+\lambda^l M)^{a^{(l)}_1}(1+\lambda^l M^2)^{a^{(l)}_2}\ldots(1+\lambda^l M^{l-1})^{a^{(l)}_{l-1}}, \quad (\mathfrak{l}^{l+1}), \end{aligned}$$

wo a eine bestimmte der Zahlen 1, 2, ..., $l-1$ und die $(l+1)(l-1)$ Exponenten $a_1, a_2, \ldots, a^{(l)}_{l-1}$ bestimmte ganze rationale Zahlen aus der Reihe 0, 1, 2, ..., $l-1$ sind. Wegen der Congruenzen (75.) und (76.) folgt daher:

$$\begin{aligned} N_k(A) \equiv a^l(1+\lambda+\lambda^2\varrho_1)^{a_1}(1+\lambda^2+\lambda^3\varrho_2)^{a_2}\ldots \\ \ldots(1+\lambda^{l-1}+\lambda^l\varrho_{l-1})^{a_{l-1}}, \quad (\mathfrak{l}^{l+1}). \end{aligned}$$

Der Ausdruck rechter Hand stellt, wenn a die Werte $1, 2, \ldots, l-1$ und die Exponenten $a_1, a_2, \ldots, a_{l-1}$ unabhängig von einander je die Werte $0, 1, 2, \ldots, l-1$ durchlaufen, genau $(l-1)l^{l-1}$ Zahlen dar, und diese sind, wie leicht ersichtlich, alle einander incongruent nach $\mathfrak{l}^{l+1}$. Nun ist jede zu $\mathfrak{l}$ prime Zahl in $k(\zeta)$, welche der Relativnorm $N_k(A)$ einer Zahl A in $k(M, \zeta)$ congruent nach $\mathfrak{l}^{l+1}$ ist, notwendig einem Ausdruck dieser Gestalt nach $\mathfrak{l}^{l+1}$ congruent, und umgekehrt ist auch jeder Ausdruck von dieser Gestalt, wie man aus (75.) entnimmt, der Relativnorm einer Zahl in $k(M, \zeta)$ nach $\mathfrak{l}^{l+1}$ congruent. Mit Hülfe der Congruenzen (73.) erkennt man, dass zwei nach $\mathfrak{l}^{l+1}$ congruente, zu $\mathfrak{l}$ prime Zahlen in $k(\zeta)$ stets gleichzeitig Normenrest oder Normennichtrest nach $\mathfrak{l}$ sind. Die Anzahl der Normenreste nach $\mathfrak{l}$, welche zu $\mathfrak{l}$ prim und untereinander incongruent nach $\mathfrak{l}^{l+1}$ sind, ist also genau gleich $(l-1)l^{l-1}$, d. i. gleich dem $l$ten Teil der nach $\mathfrak{l}^{l+1}$ möglichen incongruenten, zu $\mathfrak{l}$ primen Zahlen in $k(\zeta)$, und dieses Resultat kann sofort auf die Potenzen $\mathfrak{l}^e$ mit Exponenten $e > l+1$ ausgedehnt werden.

Von den übrigen möglichen Annahmen über μ werde hier der Kürze wegen nur die einfachste behandelt; es werde nämlich $\mu \equiv 1+\lambda$ nach $\mathfrak{l}^2$ zu Grunde gelegt. Setzen wir dann $\Omega = M-1$, so ist Ω eine durch $\mathfrak{L}$, aber nicht durch $\mathfrak{L}^2$ teilbare ganze Zahl in $k(M, \zeta)$, und wenn wir berücksichtigen, dass $N_k(\Omega) \equiv \lambda$ nach $\mathfrak{l}^2$ wird, so erkennen wir durch eine leichte Rechnung die Richtigkeit der Congruenzen

$$(77.)\quad \left\{\begin{aligned} & N_k(1+\Omega) \equiv 1+\lambda, && (\mathfrak{l}^2),\\ \text{d. i. } & N_k(1+\Omega) \equiv 1+\lambda+\lambda^2\varrho_1, && (\mathfrak{l}^l),\\ & N_k(1+\Omega^2) \equiv 1+\lambda^2, && (\mathfrak{l}^3),\\ \text{d. i. } & N_k(1+\Omega^2) \equiv 1+\lambda^2+\lambda^3\varrho_2, && (\mathfrak{l}^l),\\ & \cdots\cdots\cdots\cdots\cdots\cdots && \\ & N_k(1+\Omega^{l-2}) \equiv 1+\lambda^{l-2}, && (\mathfrak{l}^{l-1}),\\ \text{d. i. } & N_k(1+\Omega^{l-2}) \equiv 1+\lambda^{l-2}+\lambda^{l-1}\varrho_{l-2}, && (\mathfrak{l}^l),\end{aligned}\right.$$

wo $\varrho_1, \varrho_2, \ldots, \varrho_{l-2}$ gewisse ganze Zahlen in $k(\zeta)$ bedeuten. Wir haben ferner

$$N_k(1+\Omega^{l-1}) = 1+\Sigma_1+\Sigma_2+\Sigma_3+\cdots+\Sigma_{l-1}+N_k(\Omega^{l-1}),$$

wo zur Abkürzung

$$\Sigma_1 = \Omega^{l-1} + (S\Omega)^{l-1} + \cdots + (S^{l-1}\Omega)^{l-1},$$
$$\Sigma_2 = \Omega^{l-1}(S\Omega)^{l-1} + \Omega^{l-1}(S^2\Omega)^{l-1} + \cdots + (S^{l-2}\Omega)^{l-1}(S^{l-1}\Omega)^{l-1},$$
$$\Sigma_3 = \Omega^{l-1}(S\Omega)^{l-1}(S^2\Omega)^{l-1} + \cdots + (S^{l-3}\Omega)^{l-1}(S^{l-2}\Omega)^{l-1}(S^{l-1}\Omega)^{l-1},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

gesetzt ist. Nun ergiebt sich sofort $\Sigma_1 = l$. Die einzelnen Summanden in den Ausdrücken für $\Sigma_2, \Sigma_3, \ldots, \Sigma_{l-1}$ sind sämtlich jedenfalls durch $\mathfrak{L}^l$ teilbar, sie lassen sich ferner in Aggregate von je l Summanden zusammenfassen, die aus einem beliebigen unter ihnen durch die Substitutionen $1, S, S^2, \ldots, S^{l-1}$ hervorgehen; setzen wir nun ein beliebiges Glied in der Gestalt $\lambda\Phi$ an, so bedeutet Φ eine ganze Zahl in $k(M, \zeta)$ und kann daher, wie aus dem Beweise des Hülfssatzes 23 hervorgeht, als ganze rationale Function von Ω und mithin auch von M dargestellt werden, deren Coefficienten ganze oder gebrochene Zahlen in $k(\zeta)$ mit lauter zu $\mathfrak{l}$ primen Nennern sind. Setzen wir dementsprechend $\Phi = F(M)$, so lässt sich das betreffende Aggregat von l Summanden in die Form

$$\lambda\{F(M) + F(\zeta M) + F(\zeta^2 M) + \cdots + F(\zeta^{l-1} M)\}$$

bringen; die hier in der Klammer stehende Summe fällt, wie leicht ersichtlich, stets congruent 0 nach l aus; danach müssen nun die Zahlen $\Sigma_2, \Sigma_3, \ldots, \Sigma_{l-1}$ sämtlich congruent 0 nach $\mathfrak{l}^l$ sein, also wird

$$(78.) \qquad N_k(1+\Omega^{l-1}) \equiv 1 + l + \lambda^{l-1} \equiv 1, \quad (\mathfrak{l}^l).$$

Endlich ergeben sich leicht die Congruenzen

$$(79.) \qquad N_k(1+\lambda^t\Omega^g) \equiv 1, \quad (\mathfrak{l}^l)$$

für $t = 1, 2, 3, \ldots$; $g = 1, 2, 3, \ldots, l-1$.

Nun genügt offenbar jede zu $\mathfrak{L}$ prime ganze Zahl in $k(M, \zeta)$ einer Congruenz von der Gestalt

$$\begin{aligned} A \equiv a(1+\Omega)^{a_1} & (1+\Omega^2)^{a_2} \ldots (1+\Omega^{l-1})^{a_{l-1}}. \\ (1+\lambda\Omega)^{a'_1} & (1+\lambda\Omega^2)^{a'_2} \ldots (1+\lambda\Omega^{l-1})^{a'_{l-1}}. \\ & \cdots\cdots\cdots\cdots \\ (1+\lambda^{l-1}\Omega)^{a_1^{(l-1)}} & (1+\lambda^{l-1}\Omega^2)^{a_2^{(l-1)}} \ldots (1+\lambda^{l-1}\Omega^{l-1})^{a_{l-1}^{(l-1)}}, \quad (\mathfrak{l}^l), \end{aligned}$$

wo a eine der Zahlen $1, 2, \ldots, l-1$, und wo die $l(l-1)$ Exponenten

$a_1, a_2, \ldots, a_{l-1}^{(l-1)}$ bestimmte Zahlen aus der Reihe $0, 1, 2, \ldots, l-1$ sind. Wegen der vorhin aufgestellten Congruenzen (77.), (78.), (79.) folgt hieraus:

$$N_k(A) \equiv a^l(1+\lambda+\lambda^2\varrho_1)^{a_1}(1+\lambda^2+\lambda^3\varrho_2)^{a_2}\ldots$$
$$\ldots(1+\lambda^{l-2}+\lambda^{l-1}\varrho_{l-2})^{a_{l-2}}, \quad (\mathfrak{l}^l).$$

Der hier rechts stehende Ausdruck stellt nun, wenn a die Werte $1, 2, \ldots$ $\ldots, l-1$, und wenn die Exponenten $a_1, a_2, \ldots, a_{l-2}$ unabhängig von einander die Werthe $0, 1, 2, \ldots, l-1$ durchlaufen, $(l-1)l^{l-2}$ Zahlen dar, und diese sind sämtlich zu $\mathfrak{l}$ prim und einander incongruent nach $\mathfrak{l}^l$. Mit Benutzung der Congruenz $N_k(1+\lambda M) \equiv 1+\lambda^l$ nach $\mathfrak{l}^{l+1}$ und weiter der Congruenzen (73.) schliessen wir hieraus, dass genau der $l$te Teil aller zu $\mathfrak{l}$ primen und nach $\mathfrak{l}^l$ einander incongruenten Zahlen Normenreste des Körpers $k(M, \zeta)$ nach $\mathfrak{l}$ liefert, und übertragen dann dieses Resultat sogleich auf den Fall der Potenzen $\mathfrak{l}^e$ mit Exponenten $e = l+1$ bez. $e > l+1$.

Das nämliche Resultat ergiebt sich durch entsprechende Rechnungen auch dann, wenn $\mu \equiv 1$ nach $\mathfrak{l}^2$ genommen wird, und damit ist der Satz 150 in allen Teilen bewiesen. Es sei jedoch bemerkt, dass wir es in unseren späteren Entwickelungen so einrichten können, dass der Satz 150 lediglich für den oben ausführlich bewiesenen Fall $\mu \equiv 1+\lambda$ nach $\mathfrak{l}^2$ zur Verwendung gelangt.

Der Satz 150 bringt eine neue, tief eingreifende Eigenschaft der in der Relativdiscriminante des Körpers $k(M, \zeta)$ in Bezug auf $k(\zeta)$ aufgehenden Primideale $\mathfrak{w}$ zum Ausdruck. Diese Eigenschaft entspricht gewissermassen dem bekannten Satze über die Verzweigungspunkte einer Riemann'schen Fläche, wonach eine algebraische Function in der Umgebung eines Verzweigungspunktes $l$ter Ordnung den Vollwinkel auf den $l$ten Teil desselben conform abbildet. Infolgedessen nenne ich die in der Relativdiscriminante von $k(M, \zeta)$ in Bezug auf $k(\zeta)$ aufgehenden Primideale $\mathfrak{w}$ auch **Verzweigungsideale** für den Körper $k(M, \zeta)$; es bedeuten hier also „Primfactor der Relativdiscriminante", „ambiges Primideal", „Verzweigungsideal" den nämlichen Begriff.

§ 131.

Das Symbol $\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}$.

Der Satz 150 weist uns auf die Möglichkeit hin, die nach einer Potenz $\mathfrak{w}^e$ ($e > l$ im Falle $\mathfrak{w} = \mathfrak{l}$) vorhandenen, einander incongruenten Zahlen des Körpers $k(\zeta)$ in l Abteilungen zu sondern, die sämtlich gleich viele Zahlen enthalten, und von denen eine die Normenreste nach $\mathfrak{w}$ umfasst. Um diese Sonderung in übersichtlicher Weise vornehmen zu können, führe ich ein neues Symbol $\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}$ ein, welches zwei beliebigen, von 0 verschiedenen ganzen Zahlen ν, μ des Körpers $k(\zeta)$ in Bezug auf ein beliebiges Primideal $\mathfrak{w}$ in $k(\zeta)$ jedesmal eine bestimmte $l$te Einheitswurzel zuweist, und zwar geschieht dies in folgender Weise:

Es sei zunächst $\mathfrak{w}$ ein von $\mathfrak{l}$ verschiedenes Primideal. Ist dann ν genau durch $\mathfrak{w}^b$ und μ genau durch $\mathfrak{w}^a$ teilbar, so bilde man die Zahl $\varkappa = \frac{\nu^a}{\mu^b}$ und bringe $\varkappa$ in die Gestalt eines Bruches $\frac{\varrho}{\sigma}$, dessen Zähler ϱ und Nenner σ nicht durch $\mathfrak{w}$ teilbar sind. Das **Symbol** $\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}$ werde dann durch die Formel

$$\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\} = \left\{\frac{\varkappa}{\mathfrak{w}}\right\} = \left\{\frac{\varrho}{\mathfrak{w}}\right\}\left\{\frac{\sigma}{\mathfrak{w}}\right\}^{-1}$$

definirt. Es ergeben sich hieraus unmittelbar für dieses Symbol die einfachen Regeln:

$$(80.)\quad \begin{cases} \left\{\frac{\nu_1\nu_2,\mu}{\mathfrak{w}}\right\} = \left\{\frac{\nu_1,\mu}{\mathfrak{w}}\right\}\left\{\frac{\nu_2,\mu}{\mathfrak{w}}\right\}, \\ \left\{\frac{\nu,\mu_1\mu_2}{\mathfrak{w}}\right\} = \left\{\frac{\nu,\mu_1}{\mathfrak{w}}\right\}\left\{\frac{\nu,\mu_2}{\mathfrak{w}}\right\}, \\ \left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}\left\{\frac{\mu,\nu}{\mathfrak{w}}\right\} = 1, \end{cases}$$

wo ν, ν_1, ν_2, μ, μ_1, μ_2 beliebige von Null verschiedene ganze Zahlen in $k(\zeta)$ bedeuten können.

Um das neue Symbol für den Fall $\mathfrak{w} = \mathfrak{l}$ zu definiren, stellen wir folgende Ueberlegungen an:

Wenn eine beliebige ganze Zahl ω in $k(\zeta)$ vorgelegt ist, welche

der Congruenz $\omega \equiv 1$ nach $\mathfrak{l}$ genügt, und wenn wir setzen

$$\omega = c + c_1\zeta + \cdots + c_{l-2}\zeta^{l-2},$$

so dass $c, c_1, \ldots, c_{l-2}$ ganze rationale Zahlen sind, so genügen diese notwendig der Congruenz

$$c + c_1 + \cdots + c_{l-2} \equiv 1, \quad (l).$$

Setzen wir dann

$$\omega(x) = c + c_1 x + \cdots + c_{l-2}x^{l-2} - \frac{c + c_1 + \cdots + c_{l-2} - 1}{l}(1 + x + \cdots + x^{l-1}),$$

so stellt $\omega(x)$ eine ganzzahlige Function $(l-1)$ten Grades dar, und es wird

$$\omega(1) = 1 \quad \text{und} \quad \omega(\zeta) = \omega.$$

Diese Function heisse die **zur ganzen Zahl ω gehörende Function.** Wir schreiben ferner

$$(81.) \qquad \left[\frac{d^g \log \omega(e^v)}{dv^g}\right]_{v=0} = \mathrm{l}^{(g)}(\omega), \qquad (g = 1, 2, \ldots, l-1)$$

welche Verbindungen von *Kummer* mit Vorteil zur Abkürzung gewisser Rechnungen eingeführt sind. [*Kummer*[12].]

Wird die Zahl ω mit der Congruenzeigenschaft $\omega \equiv 1$ nach $\mathfrak{l}$ auf irgend eine Weise in die Gestalt

$$\omega = a + a_1\zeta + \cdots + a_t\zeta^t$$

gebracht, wo $a, a_1, \ldots, a_t$ ganze rationale Zahlen bedeuten, so stellt

$$\varpi(x) = a + a_1 x + \cdots + a_t x^t$$

eine ganzzahlige Function t-ten Grades dar, welche im allgemeinen nicht der Gleichung $\varpi(1) = 1$, aber jedenfalls der Congruenz

$$\varpi(1) \equiv 1, \quad (l)$$

Genüge leistet und also für $x = 1$ zu l prim ausfällt. Zwischen den Differentialquotienten von $\log \varpi(e^v)$ für $v = 0$ und den soeben eingeführten

Differentialquotienten (81.) bestehen folgende Congruenzen:

$$\left[\frac{d^g \log \varpi(e^v)}{d v^g}\right]_{v=0} \equiv \mathfrak{l}^{(g)}(\omega), \quad (l),$$
$$(g = 1, 2, \ldots, l-2),$$

$$\left[\frac{d^{l-1} \log \varpi(e^v)}{d v^{l-1}}\right]_{v=0} \equiv \mathfrak{l}^{(l-1)}(\omega) + \frac{1-\varpi(1)}{l}, \quad (l).$$

Die Richtigkeit dieser Congruenzen erkennen wir leicht wegen

$$\omega(x) = \varpi(x) + \frac{1-\varpi(1)}{l}(1+x+\cdots+x^{l-1}) + O(x)(x^l-1),$$

$$\omega(e^v) \equiv \varpi(e^v) + \frac{1-\varpi(1)}{l} v^{l-1}, \quad (l);$$

in der ersten Formel bedeutet $O(x)$ eine bestimmte ganzzahlige Function von x, und die zweite Formel soll besagen, dass in den Entwickelungen der beiden Seiten dieser Congruenz nach Potenzen von v die Coefficienten von $1, v, v^2, \ldots, v^{l-1}$ nach l congruent ausfallen.

Sind ν, μ irgend zwei ganze Zahlen in $k(\zeta)$ mit der Congruenzeigenschaft $\nu \equiv 1$, $\mu \equiv 1$ nach $\mathfrak{l}$, so definiren wir das **Symbol** $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ wie folgt:

$$(82.) \quad \left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = \zeta^{\mathfrak{l}^{(1)}(\nu)\mathfrak{l}^{(l-1)}(\mu) - \mathfrak{l}^{(2)}(\nu)\mathfrak{l}^{(l-2)}(\mu) + \cdots - \mathfrak{l}^{(l-1)}(\nu)\mathfrak{l}^{(1)}(\mu)}.$$

Aus dieser Definition ergeben sich unmittelbar die folgenden Regeln:

$$(83.) \quad \begin{cases} \left\{\frac{\nu_1\nu_2, \mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu_1, \mu}{\mathfrak{l}}\right\}\left\{\frac{\nu_2, \mu}{\mathfrak{l}}\right\}, \\ \left\{\frac{\nu, \mu_1\mu_2}{\mathfrak{l}}\right\} = \left\{\frac{\nu, \mu_1}{\mathfrak{l}}\right\}\left\{\frac{\nu, \mu_2}{\mathfrak{l}}\right\}, \\ \left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}\left\{\frac{\mu, \nu}{\mathfrak{l}}\right\} = 1, \end{cases}$$

wo $\nu, \nu_1, \nu_2, \mu, \mu_1, \mu_2$ beliebige ganze Zahlen $\equiv 1$ nach $\mathfrak{l}$ in $k(\zeta)$ bedeuten können. Bezeichnet r eine Primitivzahl nach l und $s = (\zeta : \zeta^r)$ die entsprechende Substitution der Gruppe des Kreiskörpers $k(\zeta)$, so gilt, wie leicht ersichtlich ist, die weitere Formel

$$(84.) \quad \left\{\frac{s\nu, s\mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}^r.$$

Sind ν, μ beliebige zu $\mathfrak{l}$ prime ganze Zahlen des Körpers $k(\zeta)$, so definire ich das **Symbol** $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ durch die Formel

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu^{l-1}, \mu^{l-1}}{\mathfrak{l}}\right\}.$$

Für den Fall, dass eine der Zahlen ν, μ oder beide durch $\mathfrak{l}$ teilbar sind, vergleiche man die Bemerkungen gegen Schluss des § 133.

§ 132.

Einige Hülfssätze über das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ und über Normenreste nach dem Primideal $\mathfrak{l}$.

Hülfssatz 24. Wenn ω eine ganze Zahl in $k(\zeta)$ mit der Congruenzeigenschaft $\omega \equiv 1$ nach $\mathfrak{l}$ ist, so gilt für die Norm $n(\omega)$ von ω in $k(\zeta)$ die Congruenz

$$1^{(l-1)}(\omega) \equiv \frac{1-n(\omega)}{l}, \quad (l).$$

[*Kummer*[20].]

Beweis. Es bedeute $\omega(x)$ die zu ω gehörende Function, und es werde

$$F(x) = \prod_{(g)} \omega(1+x(\zeta^g-1))$$

gesetzt, wo das Product über die Werte $g = 0, 1, 2, \ldots, l-1$ zu erstrecken ist. Der Ausdruck $F(x)$ stellt eine ganzzahlige Function von x dar, und die Coefficienten aller durch x^l teilbaren Glieder dieser Function sind offenbar durch λ^l und folglich wegen der Rationalität der Coefficienten auch durch l^2 teilbar. Durch Entwickelung nach Potenzen von x ergiebt sich nun:

$$(85.)\quad \begin{cases} \log\omega(1+x(\xi-1)) = \dfrac{\xi-1}{1!}\, x \left[\dfrac{\mathrm{d}\log\omega(x)}{\mathrm{d}x}\right]_{x=1} \\[2ex] \qquad + \dfrac{(\xi-1)^2}{2!}\, x^2 \left[\dfrac{\mathrm{d}^2\log\omega(x)}{\mathrm{d}x^2}\right]_{x=1} + \cdots \\[2ex] \qquad \cdots + \dfrac{(\xi-1)^{l-1}}{l-1!}\, x^{l-1} \left[\dfrac{\mathrm{d}^{l-1}\log\omega(x)}{\mathrm{d}x^{l-1}}\right]_{x=1} + \cdots. \end{cases}$$

Setzen wir erstens in dieser Entwickelung der Reihe nach

$$\xi = 1,\ \ \zeta,\ \ \zeta^2,\ \ \ldots,\ \ \zeta^{l-1}$$

ein und addiren die betreffenden Formeln, so entsteht unter Berück-

sichtigung von

$$(\zeta-1)^g+(\zeta^2-1)^g+\cdots+(\zeta^{l-1}-1)^g = (-1)^g l \qquad (g=1,2,\ldots,l-1)$$

die Gleichung:

$$(86.)\quad \begin{cases} \log F(x) = l\Big\{-\frac{x}{1!}\left[\frac{\mathrm{d}\log\omega(x)}{\mathrm{d}x}\right]_{x=1} \\ \qquad +\frac{x^2}{2!}\left[\frac{\mathrm{d}^2\log\omega(x)}{\mathrm{d}x^2}\right]_{x=1}-\cdots \\ \qquad \cdots+\frac{x^{l-1}}{l-1!}\left[\frac{\mathrm{d}^{l-1}\log\omega(x)}{\mathrm{d}x^{l-1}}\right]_{x=1}\Big\}+x^l G, \end{cases}$$

wobei $x^l G$ das Aggregat der durch x^l teilbaren Glieder der Entwickelung andeutet.

Setzen wir zweitens in der Entwickelung (85.) $\xi = \mathrm{e}^v$ ein und bilden den $(l-1)$ten Differentialquotienten nach v, so wird derselbe für $v=0$:

$$(87.)\quad \begin{cases} \left[\frac{\mathrm{d}^{l-1}\log\omega(1+x(\mathrm{e}^v-1))}{\mathrm{d}v^{l-1}}\right]_{v=0} = \frac{x}{1!}\left[\frac{\mathrm{d}\log\omega(x)}{\mathrm{d}x}\right]_{x=1} \\ \qquad +\frac{2^{l-1}-2.1^{l-1}}{2!}x^2\left[\frac{\mathrm{d}^2\log\omega(x)}{\mathrm{d}x^2}\right]_{x=1} \\ \qquad +\frac{3^{l-1}-3.2^{l-1}+3.1^{l-1}}{3!}x^3\left[\frac{\mathrm{d}^3\log\omega(x)}{\mathrm{d}x^3}\right]_{x=1} \\ \qquad +\frac{(l-1)^{l-1}-\cdots-(l-1)1^{l-1}}{l-1!}x^{l-1}\left[\frac{\mathrm{d}^{l-1}\log\omega(x)}{\mathrm{d}x^{l-1}}\right]_{x=1} \\ \qquad \equiv \frac{x}{1!}\left[\frac{\mathrm{d}\log\omega(x)}{\mathrm{d}x}\right]_{x=1}-\frac{x^2}{2!}\left[\frac{\mathrm{d}^2\log\omega(x)}{\mathrm{d}x^2}\right]_{x=1}+\cdots \\ \qquad \cdots-\frac{x^{l-1}}{l-1!}\left[\frac{\mathrm{d}^{l-1}\log\omega(x)}{\mathrm{d}x^{l-1}}\right]_{x=1}, \quad (l). \end{cases}$$

Durch Vergleichung der beiden Formeln (86.) und (87.) ergiebt sich

$$\log F(x) \equiv -l\left[\frac{\mathrm{d}^{l-1}\log\omega(1+x(\mathrm{e}^v-1))}{\mathrm{d}v^{l-1}}\right]_{v=0}, \quad (l^2),$$

d. h. die Coefficienten von $x, x^2, \ldots, x^{l-1}$ auf der linken Seite sind den entsprechenden Coefficienten rechts nach l^2 congruent, und wenn wir beide Seiten dieser Congruenz in den Exponenten von e setzen, so

erhalten wir zunächst in demselben Sinne, dann aber mit Rücksicht auf die zu Beginn dieses Beweises gemachte Bemerkung auch vollständig die Congruenz der zwei ganzzahligen Functionen:

$$F(x) \equiv 1 - l\left[\frac{\mathrm{d}^{l-1}\log\omega(1+x(\mathrm{e}^v-1))}{\mathrm{d}v^{l-1}}\right]_{v=0}, \quad (l^2),$$

und folglich für $x=1$:

$$n(\omega) \equiv 1 - l.\mathrm{l}^{(l-1)}(\omega), \quad (l^2),$$

womit der Hülfssatz 24 bewiesen ist.

Hülfssatz 25. Wenn die ganzen Zahlen ν, μ in $k(\zeta)$ die Congruenzeigenschaften $\nu \equiv 1$ nach $\mathfrak{l}$ und $\mu \equiv 1+\lambda$ nach $\mathfrak{l}^2$ besitzen, und wenn ausserdem ν congruent der Relativnorm einer ganzen Zahl A des durch $M=\sqrt[l]{\mu}$ bestimmten Kummer'schen Körpers $k(M,\zeta)$ nach $\mathfrak{l}^l$ ist, so existirt eine ganzzahlige Function $f(x)$ vom $(l-1)$ten Grade in x, derart, dass $f(1)>0$ ist und die Congruenzen

$$n(f(\zeta)) \equiv 1, \quad (l^2)$$

und

$$\nu \equiv f(\mu), \quad (\mathfrak{l}^l)$$

erfüllt sind. [*Kummer*[20].]

Beweis. Nach dem Beweise des Hülfssatzes 23 ist jede ganze Zahl A in $k(M,\zeta)$ in der Gestalt

$$A = \frac{\gamma+\gamma_1(M-1)+\cdots+\gamma_{l-1}(M-1)^{l-1}}{\delta}$$

und folglich auch in der Gestalt

$$A = \frac{\beta+\beta_1 M+\cdots+\beta_{l-1}M^{l-1}}{\delta}$$

darstellbar, so dass $\gamma, \gamma_1, \ldots, \gamma_{l-1}$, δ und $\beta, \beta_1, \ldots, \beta_{l-1}$ ganze Zahlen in $k(\zeta)$ sind und überdies δ zu $\mathfrak{l}$ prim ausfällt. Infolge des letzteren Umstandes können wir

$$A \equiv \alpha+\alpha_1 M+\cdots+\alpha_{l-1}M^{l-1}, \quad (\mathfrak{l}^l)$$

setzen in solcher Weise, dass $\alpha, \alpha_1, \ldots, \alpha_{l-1}$ ganze Zahlen in $k(\zeta)$ sind. Es sei nun

$$\alpha \equiv a^*, \quad \alpha_1 \equiv a_1^*, \quad \ldots, \quad \alpha_{l-1} \equiv a_{l-1}^*, \quad (\mathfrak{l}),$$

wo a^*, a, ..., a_{l-1}^* ganze rationale positive Zahlen bedeuten sollen; wir

setzen

$$f^*(x) = a^* + a_1^* x + \cdots + a_{l-1}^* x^{l-1}.$$

Da in $k(M, \zeta)$ sich $\mathfrak{l} = \mathfrak{L}^l$ und $M \equiv 1$ nach $\mathfrak{L}$ erweist, so folgt

$$A \equiv \alpha + \alpha_1 + \cdots + \alpha_{l-1} \equiv a^* + a_1^* + \cdots + a_{l-1}^*, \quad (\mathfrak{L}).$$

Ist nun A die vorausgesetzte Zahl, für welche $N_k(A) \equiv \nu$ nach $\mathfrak{l}^l$ wird, so erhalten wir weiter

$$\nu \equiv N_k(A) \equiv a^* + a_1^* + \cdots + a_{l-1}^* \equiv 1, \quad (\mathfrak{L})$$

also auch

$$(88.) \qquad a^* + a_1^* + \cdots + a_{l-1}^* \equiv 1, \quad (l).$$

Folglich ist $f^*(\zeta)$ eine Zahl in $k(\zeta)$ mit der Congruenzeigenschaft $f^*(\zeta) \equiv 1$ nach $\mathfrak{l}$. Wir finden nun mit Rücksicht hierauf leicht eine ganze rationale positive Zahl b derart, dass die Norm der Zahl $f(\zeta) = f^*(\zeta) + lb$ im Körper $k(\zeta)$ der Congruenz

$$(89.) \qquad n(f(\zeta)) \equiv 1, \quad (l^2)$$

genügt; dann erfüllt die ganzzahlige Function

$$f(x) = f^*(x) + lb = a + a_1 x + \cdots + a_{l-1} x^{l-1}$$

die Bedingungen des zu beweisenden Hülfssatzes 25. Denn es ist offenbar $A = f(M) + \lambda B$, wo B eine ganze Zahl in $k(M, \zeta)$ bedeutet. Hieraus ergiebt sich leicht durch eine ähnliche Betrachtung wie auf S. 409:

$$(90.) \qquad \nu \equiv N_k(A) \equiv N_k(f(M)), \quad (\mathfrak{l}^l).$$

Andererseits erkennen wir unter Berücksichtigung der Congruenzen

$$a^l \equiv a, \quad a_1^l \equiv a_1, \quad \ldots, \quad a_{l-1}^l \equiv a_{l-1}, \quad (l),$$

dass identisch in x eine Gleichung

$$(91.) \qquad f(x) f(\zeta x) \ldots f(\zeta^{l-1} x) = f(x^l) + l F(x^l)$$

gilt, wo $F(x^l)$ eine ganzzahlige Function von x^l bedeutet. Diese Gleichung liefert für $x = 1$ mit Rücksicht auf (89.) die Congruenz

$$f(1) \equiv f(1) + l F(1), \quad (l^2), \qquad \text{d. h.} \qquad F(1) \equiv 0, \quad (l).$$

Wenn in der Gleichung (91.) $x = M$ genommen wird, so ergiebt sich

$$N_k(f(M)) = f(\mu) + l F(\mu)$$

und hieraus, da $F(\mu) \equiv F(1) \equiv 0$ nach $\mathfrak{l}$ ausfällt,

$$N_k(f(M)) \equiv f(\mu), \quad (\mathfrak{l}^l),$$

d. i. wegen (90.)

$$\nu \equiv f(\mu), \quad (\mathfrak{l}^l).$$

Damit und in Anbetracht von (89.) ist der Hülfssatz 25 vollständig bewiesen.

Hülfssatz 26. Wenn ν, μ ganze Zahlen in $k(\zeta)$ mit den Congruenzeigenschaften $\nu \equiv 1$ nach $\mathfrak{l}$ und $\mu \equiv 1+\lambda$ nach $\mathfrak{l}^2$ bedeuten, und wenn ausserdem ν Normenrest des durch $M = \sqrt[l]{\mu}$ bestimmten Kummer'schen Körpers $k(M, \zeta)$ nach $\mathfrak{l}$ ist, so wird stets

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = 1.$$

[*Kummer*[20].]

Beweis. Aus der bekannten Lagrange'schen Formel für die Umkehrung einer Potenzreihe entnimmt man unmittelbar die folgende Identität:

$$(92.) \quad \left[\frac{\mathrm{d}^{l-1} F(v)}{\mathrm{d} V^{l-1}}\right]_{V=0} = \left[\frac{\mathrm{d}^{l-2} \dfrac{\mathrm{d}F(v)}{\mathrm{d}v} (\varphi(v))^{l-1}}{\mathrm{d}v^{l-2}}\right]_{v=0};$$

dabei stelle man sich unter $F(v)$ eine beliebige Potenzreihe von v, ferner unter $\varphi(v)$ eine Potenzreihe vor, deren constantes Glied von 0 verschieden ist, und denke sich den Zusammenhang der Variabeln v und V durch die Gleichung $V\varphi(v) - v = 0$ vermittelt.

Es seien nun $\nu(x)$ und $\mu(x)$ die zu den Zahlen ν und μ gehörenden Functionen. Da ν Normenrest des Körpers $k(M, \zeta)$ nach $\mathfrak{l}$ sein soll, so giebt es nach Hülfssatz 25 eine ganzzahlige Function $(l-1)$ten Grades $f(x)$ derart, dass

$$(93.) \quad n(f(\zeta)) \equiv 1, \quad (l^2),$$

$$(94.) \quad \nu \equiv f(\mu), \quad (\mathfrak{l}^l)$$

und $f(1) > 0$ wird.

Wir setzen nun

$$F(v) = \log f(\mu(\mathrm{e}^v)),$$

$$V = \log \mu(\mathrm{e}^v),$$

$$\varphi(v) = \frac{v}{\log \mu(\mathrm{e}^v)};$$

diese Functionen werden nur an der Stelle $v = 0$ betrachtet werden, und es sollen die Logarithmen so genommen werden, dass sie für $v = 0$ reell sind.

Ersetzen wir die Zeichen ω, $\varpi(x)$, v in der zweiten Formel auf S. 413 oben bez. durch $f(\zeta)$, $f(x)$, V, so wird aus derselben

$$\left[\frac{\mathrm{d}^{l-1}\log f(e^V)}{\mathrm{d}V^{l-1}}\right]_{V=0} \equiv \mathfrak{l}^{(l-1)}(f(\zeta))+\frac{1-f(1)}{l},\quad (l).$$

Aus Hülfssatz 24 ergiebt sich unter Berücksichtigung von (93.) die Congruenz

$$\mathfrak{l}^{(l-1)}(f(\zeta)) \equiv 0,\quad (l)$$

und folglich wird

$$(95.)\quad \left[\frac{\mathrm{d}^{l-1}F(v)}{\mathrm{d}V^{l-1}}\right]_{V=0} = \left[\frac{\mathrm{d}^{l-1}\log f(e^V)}{\mathrm{d}V^{l-1}}\right]_{V=0} \equiv \frac{1-f(1)}{l},\quad (l).$$

Andererseits gilt mit Rücksicht auf (94.) die Congruenz

$$f(\mu(e^v)) \equiv \nu(e^v)+\frac{f(1)-1}{l}v^{l-1},\quad (l),$$

welche so aufzufassen ist, dass in den Entwickelungen nach Potenzen von v die Coefficienten von $1, v, \ldots, v^{l-1}$ auf den beiden Seiten einander nach l congruent sind, und hieraus ergiebt sich die Entwickelung

$$(96.)\quad \begin{cases} \dfrac{\mathrm{d}F(v)}{\mathrm{d}v} \equiv \mathfrak{l}^{(1)}(\nu)+\mathfrak{l}^{(2)}(\nu)\dfrac{v}{1!}+\mathfrak{l}^{(3)}(\nu)\dfrac{v^2}{2!}+\cdots \\ \qquad\cdots+\left(\mathfrak{l}^{(l-1)}(\nu)+\dfrac{1-f(1)}{l}\right)\dfrac{v^{l-2}}{(l-2)!},\quad (l), \end{cases}$$

welche so aufzufassen ist, dass die Coefficienten von $1, v, \ldots, v^{l-2}$ auf den beiden Seiten einander nach l congruent sind.

Endlich betrachten wir die Function $\varphi(v)$. Wegen $\mu \equiv 1+\lambda$ nach $\mathfrak{l}^2$ wird $\varphi(v)$ eine Potenzreihe, deren constantes Glied $\equiv -1$ nach l ist. Ferner folgt leicht

$$(\varphi(v))^l \equiv \varphi(v^l) \equiv \varphi(0) \equiv -1,\quad (l)$$

in dem Sinne, dass die Coefficienten von $1, v, \ldots, v^{l-2}$ auf den beiden Seiten einander nach l congruent sind. Es gilt daher weiter in demselben Sinne

$$-(\varphi(v))^{l-1} \equiv \frac{\log\mu(e^v)}{v},\quad (l),$$

und es folgt hieraus endlich in eben demselben Sinne die Entwickelung

$$(97.)\quad \begin{cases} -(\varphi(v))^{l-1} \equiv \mathfrak{l}^{(1)}(\mu)+\mathfrak{l}^{(2)}(\mu)\dfrac{v}{2!}+\mathfrak{l}^{(3)}(\mu)\dfrac{v^2}{3!}+\cdots \\ \qquad\cdots+\mathfrak{l}^{(l-1)}(\mu)\dfrac{v^{l-2}}{(l-1)!},\quad (l). \end{cases}$$

Die Zusammenstellung der Congruenz (95.) und der beiden Entwickelungen (96.), (97.) mit (92.) liefert, wegen $\mathfrak{l}^{(1)}(\mu) \equiv -1$ und $(l-g)!(g-1)! \equiv (-1)^g$ nach l für $g = 1, 2, \ldots, l-1$, die folgende Congruenz:

$$\mathfrak{l}^{l-1}(\nu)\mathfrak{l}^{(1)}(\mu) - \mathfrak{l}^{(l-2)}(\nu)\mathfrak{l}^{(2)}(\mu) + \cdots - \mathfrak{l}^{(1)}(\nu)\mathfrak{l}^{(l-1)}(\mu) \equiv 0, \quad (\mathfrak{l}),$$

d. i. nach der Definition (82.) des Symbols $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ in § 131:

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = 1,$$

und hiermit ist der Hülfssatz 26 bewiesen.

§ 133.

Das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$ zur Unterscheidung zwischen Normenresten und Normennichtresten.

Wir sind jetzt in den Stand gesetzt, soweit die betreffenden Symbole bereits definirt sind, die Richtigkeit der folgenden Behauptung einzusehen:

Satz 151. Wenn ν, μ zwei beliebige ganze Zahlen in $k(\zeta)$ sind, nur dass $\sqrt[l]{\mu}$ nicht in $k(\zeta)$ liegt, und wenn $\mathfrak{w}$ ein beliebiges Primideal des Kreiskörpers $k(\zeta)$ bedeutet, so ist ν Normenrest oder Normennichtrest des durch $M = \sqrt[l]{\mu}$ bestimmten Kummer'schen Körpers $k(M, \zeta)$ nach $\mathfrak{w}$, je nachdem

$$\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = 1 \quad \text{oder} \quad \neq 1$$

ausfällt.

Beweis. Es sei zunächst das Primideal $\mathfrak{w}$ von $\mathfrak{l}$ verschieden und gehe nicht in der Relativdiscriminante des Körpers $k(M, \zeta)$ auf. Ist μ^* eine ganze Zahl in $k(\zeta)$ derart, dass $\frac{\mu^*}{\mu}$ die $l$te Potenz einer Zahl in $k(\zeta)$ ist, so gilt stets $\left\{\frac{\nu, \mu^*}{\mathfrak{w}}\right\} = \left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$; danach und mit Rücksicht auf Satz 148 können wir hier annehmen, dass μ nicht durch $\mathfrak{w}$ teilbar ist. Wir unterscheiden zwei Fälle, je nachdem $\mathfrak{w}$ im Körper $k(M, \zeta)$ als Product von l Primidealen $\mathfrak{W}_1, \ldots, \mathfrak{W}_l$ darstellbar wird oder in

$k(M, \zeta)$ Primideal bleibt. Nach Satz 149 ist im ersteren Falle $\left\{\frac{\mu}{\mathfrak{w}}\right\} = 1$, im letzteren $\left\{\frac{\mu}{\mathfrak{w}}\right\} \neq 1$ und $\neq 0$.

Im ersteren Falle bestimmen wir eine ganze Zahl A in $k(M, \zeta)$, welche durch $\mathfrak{W}_1$, aber nicht durch $\mathfrak{W}_1^2$ und auch nicht durch eines der Primideale $\mathfrak{W}_2, \ldots, \mathfrak{W}_l$ teilbar ist; dann geht in der Relativnorm $\alpha = N_k(A)$ das Primideal $\mathfrak{w}$ genau zur ersten Potenz auf. Ist nun $\mathfrak{w}^b$ die in ν enthaltene Potenz von $\mathfrak{w}$, so lässt sich $\varkappa = \frac{\nu}{\alpha^b}$ als ein Bruch schreiben, dessen Zähler und Nenner zu $\mathfrak{w}$ prim sind, und folglich sind Zähler und Nenner dieses Bruches nach Satz 150 Normenreste des Körpers $k(M, \zeta)$ nach $\mathfrak{w}$. Das Gleiche gilt also auch von ν. Da nach der Definition in § 131

$$\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = \left\{\frac{\mu^b}{\mathfrak{w}}\right\}^{-1} = 1$$

ist, so erweist sich im ersteren Falle der Satz 151 als richtig.

Im zweiten Falle ist die Relativnorm einer ganzen Zahl A in $k(M, \zeta)$ jedesmal genau durch eine solche Potenz von $\mathfrak{w}$ teilbar, deren Exponent ein Vielfaches von l ist. Es sei wiederum $\mathfrak{w}^b$ die in ν enthaltene Potenz von $\mathfrak{w}$; ist dann b kein Vielfaches von l, so kann also ν nicht Normenrest nach $\mathfrak{w}$ sein; in diesem Falle wird andererseits $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = \left\{\frac{\mu^b}{\mathfrak{w}}\right\}^{-1} \neq 1$. Ist dagegen b ein Vielfaches von l, und bedeutet α eine ganze durch $\mathfrak{w}$, aber nicht durch $\mathfrak{w}^2$ teilbare Zahl in $k(\zeta)$, so setzen wir $\varkappa = \frac{\nu}{\alpha^b}$ und erkennen, wie im ersteren Falle ν als Normenrest nach $\mathfrak{w}$; andererseits ist jetzt

$$\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = \left\{\frac{\mu^b}{\mathfrak{w}}\right\}^{-1} = 1.$$

Damit ist der Satz 151 auch für den zweiten Fall bewiesen.

Wir nehmen jetzt an, es sei die Relativdiscriminante des Körpers $k(M, \zeta)$ durch das Primideal $\mathfrak{w}$ teilbar; $\mathfrak{w}$ soll dabei von $\mathfrak{l}$ verschieden sein. Es gehe $\mathfrak{w}$ in ν genau zur $b$ten und in μ genau zur $a$ten Potenz auf; dann ist a jedenfalls kein Vielfaches von l. Die Zahl $\varkappa = \frac{\nu^a}{\mu^b}$ lässt sich in die Gestalt eines Bruches $\frac{\varrho}{\sigma}$ setzen, dessen Zähler ϱ und dessen Nenner σ zu $\mathfrak{w}$ prim sind. Die Zahl $\varrho\sigma^{l-1}$ ist eine nicht durch $\mathfrak{w}$ teilbare ganze Zahl; nach dem Beweise des Satzes 150 auf S. 406 ist

eine solche ganze Zahl dann und nur dann Normenrest des Körpers $k(M, \zeta)$ nach $\mathfrak{w}$, wenn sie $l$ter Potenzrest nach $\mathfrak{w}$ ist, d. i. hier, wenn $\left\{\frac{\varrho\sigma^{l-1}}{\mathfrak{w}}\right\} = 1$ und also $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = 1$ ist; damit ist für den gegenwärtigen Fall wiederum der Satz 151 als richtig erkannt.

Es sei endlich $\mathfrak{w} = \mathfrak{l}$. Wir fassen lediglich den Fall ins Auge, dass $\mu \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ ist: es ist dies der einzige Fall, für den wir die betreffenden Sätze späterhin brauchen werden; die anderen Fälle gestatten übrigens eine ähnliche Behandlung. Beim Beweise machen wir noch die nicht wesentlich einschränkende Annahme $\nu \equiv 1$ nach $\mathfrak{l}$. Wegen der Annahme $\mu \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ kann man laut Satz 150 genau l^{l-1} Normenreste ν^* des Körpers $k(M, \zeta)$ nach $\mathfrak{l}$ bilden, welche congruent 1 nach $\mathfrak{l}$ ausfallen und unter einander nach $\mathfrak{l}^{l+1}$ incongruent sind. Andererseits muss ein jeder Normenrest ν^* von $k(M, \zeta)$ nach $\mathfrak{l}$, für den man $\nu^* \equiv 1$ nach $\mathfrak{l}$ hat, laut Hülfssatz 26 die Bedingung $\left\{\frac{\nu^*, \mu}{\mathfrak{l}}\right\} = 1$ erfüllen. Wegen

$$\left.\begin{aligned} &1^{(1)}(\mu) \equiv -1, \\ &1^{(1)}(1-l) \equiv 0, \quad 1^{(2)}(1-l) \equiv 0, \quad \ldots, \quad 1^{(l-2)}(1-l) \equiv 0, \\ &1^{(l-1)}(1-l) \equiv \frac{1-n(1-l)}{l} \equiv -1, \end{aligned}\right\} \quad (l)$$

ergiebt sich nach (82.)

$$(98.) \qquad \left\{\frac{1-l, \mu}{\mathfrak{l}}\right\} = \zeta^{-1}.$$

Es sei nun α irgend eine erste ganze Zahl in $k(\zeta)$ mit der Congruenzeigenschaft $\alpha \equiv 1$ nach $\mathfrak{l}$, und es werde $\left\{\frac{\alpha, \mu}{\mathfrak{l}}\right\} = \zeta^a$ gesetzt, wo a eine Zahl aus der Reihe $0, 1, 2, \ldots, l-1$ bedeuten soll; dann ist offenbar $\left\{\frac{\alpha(1-l)^a, \mu}{\mathfrak{l}}\right\} = 1$; dagegen fällt jedesmal $\left\{\frac{\alpha(1-l)^x, \mu}{\mathfrak{l}}\right\} \neq 1$ aus, wenn x eine von a verschiedene Zahl aus der Reihe $0, 1, 2, \ldots, l-1$ bedeutet. Wählen wir ferner eine ganze Zahl α' in $k(\zeta)$, welche ebenfalls congruent 1 nach $\mathfrak{l}$, aber keiner der l Zahlen $\alpha, \alpha(1-l), \alpha(1-l)^2, \ldots, \alpha(1-l)^{l-1}$ nach $\mathfrak{l}^{l+1}$ congruent ist, so sind auch die l Zahlen $\alpha', \alpha'(1-l), \alpha'(1-l)^2, \ldots, \alpha'(1-l)^{l-1}$ nach $\mathfrak{l}^{l+1}$ sämtlich unter einander incongruent und zugleich keiner der ersteren l Zahlen congruent; unter den letzteren l Zahlen giebt es wegen (98.) offenbar eine und nur eine Zahl — es sei dies

etwa $\alpha'(1-l)^{a'}$ — von der Art, dass $\left\{\frac{\alpha'(1-l)^{a'}, \mu}{\mathfrak{l}}\right\} = 1$ ist. Fahren wir in dieser Weise fort, so erkennen wir, dass die Anzahl der vorhandenen nach $\mathfrak{l}^{l+1}$ incongruenten Zahlen ν, die congruent 1 nach $\mathfrak{l}$ sind und der Bedingung $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = 1$ genügen, genau gleich l^{l-1} ist, und aus der Uebereinstimmung dieser Anzahl mit der oben gefundenen für die Normenreste ν^* ist ersichtlich, dass umgekehrt auch jede Zahl ν mit diesen zwei Eigenschaften Normenrest des Körpers $k(M, \zeta)$ nach $\mathfrak{l}$ ist.

Durch die bisherigen Ueberlegungen ist der Satz 151 in allen Teilen bewiesen; für den Fall $\mathfrak{w} = \mathfrak{l}$ allerdings nur soweit, als für die Zahlen ν, μ die Congruenzeigenschaften $\nu \equiv 1$ nach $\mathfrak{l}$ und $\mu \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ erfüllt sind. Die ν betreffende Einschränkung ist offenbar leicht aufzuheben.

Aus dem Satze 151 folgt, bei Benutzung der ersten Formel in (80.) und (83.), die Formel

$$\left\{\frac{\nu\nu^*, \mu}{\mathfrak{w}}\right\} = \left\{\frac{\nu, \mu}{\mathfrak{w}}\right\},$$

wo $\mathfrak{w}$ ein beliebiges Primideal in $k(\zeta)$ bedeutet und ν^* ein Normenrest des Körpers $k(M, \zeta)$ nach $\mathfrak{w}$ sein soll.

Um nun das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ auch für den Fall zu definiren, dass eine der beiden Zahlen ν, μ oder beide durch $\mathfrak{l}$ theilbar sind, braucht man nur die allgemeine Gültigkeit der Formeln

$$\left\{\frac{\nu\nu^*, \mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}, \quad \left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}\left\{\frac{\mu, \nu}{\mathfrak{l}}\right\} = 1$$

festzusetzen, wobei ν^* ein beliebiger Normenrest des Körpers $k(\sqrt[l]{\mu}, \zeta)$ nach $\mathfrak{l}$ bedeuten soll. Bei dieser Festsetzung folgt dann insbesondere

$$\left\{\frac{1+a\lambda^l, \lambda}{\mathfrak{l}}\right\} = \left\{\frac{1+a\lambda^l}{\mathfrak{l}}\right\} = \zeta^a.$$

Wir können überhaupt die Definition des **Symbols** $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ auf die Formeln

$$\left\{\frac{\alpha, \zeta}{\mathfrak{l}}\right\} = \zeta^{\frac{n(\alpha)-1}{l}}, \quad \left\{\frac{\nu_1\nu_2, \mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu_1, \mu}{\mathfrak{l}}\right\}\left\{\frac{\nu_2, \mu}{\mathfrak{l}}\right\},$$

$$\left\{\frac{\nu^*, \mu}{\mathfrak{l}}\right\} = 1, \quad \left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}\left\{\frac{\mu, \nu}{\mathfrak{l}}\right\} = 1$$

gründen, wo α eine zu $\mathfrak{l}$ prime ganze Zahl in $k(\zeta)$, ν^* ein Normenrest des Körpers $k(\sqrt[l]{\mu}, \zeta)$ nach $\mathfrak{l}$ und ν, ν_1, ν_2, μ beliebige ganze Zahlen in $k(\zeta)$ sein sollen (vgl. § 166). Ich habe jedoch gegenwärtig die obige Definition (82.) gewählt, welche unmittelbar an die Entwickelungen von *Kummer* anknüpft.

Schliesslich sei hier bemerkt, dass nunmehr das zu Anfang des § 131 gesteckte Ziel erreicht ist; wenn nämlich $\mathfrak{w}^e$ eine beliebige Potenz eines Primideals $\mathfrak{w}$ bedeutet, wobei im Falle $\mathfrak{w} = \mathfrak{l}$ der Exponent $e > l$ sei, so kann offenbar ein vollständiges System zu $\mathfrak{w}$ primer und nach $\mathfrak{w}^e$ incongruenter Zahlen ν in $k(\zeta)$ mit Rücksicht auf die Werte, die das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$ annimmt, in l Abteilungen von gleich vielen Zahlen gesondert werden, von denen die eine Abteilung die sämtlichen im System befindlichen Normenreste des Kummer'schen Körpers $k(M, \zeta)$ nach $\mathfrak{w}$ darstellt.

Capitel XXX.

Das Vorhandensein unendlich vieler Primideale mit vorgeschriebenen Potenzcharakteren im Kummer'schen Körper.

§ 134.

Der Grenzwert eines gewissen unendlichen Productes.

Nachdem wir in § 128 die Primideale des Kummer'schen Körpers sämtlich aufgestellt haben, sind wir im Stande, diejenigen Untersuchungen für den Kummer'schen Körper durchzuführen, welche den in § 79 und in § 80 für den quadratischen Körper behandelten Fragen entsprechen. Wir leiten vor allem die folgende wichtige Thatsache ab:

Hülfssatz 27. Bedeutet l eine ungerade rationale Primzahl und α in dem durch $\zeta = e^{\frac{2i\pi}{l}}$ bestimmten Kreiskörper $k(\zeta)$ eine beliebige ganze Zahl, nur nicht die $l$te Potenz einer in $k(\zeta)$ liegenden Zahl, so ist der Grenzwert

$$\underset{s=1}{L} \prod_{(\mathfrak{p})} \prod_{(m)} \frac{1}{1 - \left\{\frac{\alpha}{\mathfrak{p}}\right\}^m n(\mathfrak{p})^{-s}}$$

stets eine endliche und von 0 verschiedene Grösse; dabei soll das Product $\prod\limits_{(\mathfrak{p})}$ über alle Primideale $\mathfrak{p}$ des Körpers $k(\zeta)$ und das Product $\prod\limits_{(m)}$

über alle Exponenten m aus der Reihe 1, 2, ..., $l-1$ erstreckt werden. [*Kummer*[20].]

Beweis. Fassen wir den durch $\sqrt[l]{\alpha}$ und ζ bestimmten Kummer'schen Körper $K = k(\sqrt[l]{\alpha}, \zeta)$ in's Auge und bezeichnen wir die dem Satze 56 gemäss gebildete Function $\zeta(s)$ für denselben mit $\zeta_K(s)$, so ist nach § 27

$$\zeta_K(s) = \prod_{(\mathfrak{P})} \frac{1}{1-N(\mathfrak{P})^{-s}},$$

wo das Product über alle Primideale $\mathfrak{P}$ in K zu erstrecken ist und $N(\mathfrak{P})$ die in K genommene Norm von $\mathfrak{P}$ bedeutet. Ordnen wir dieses Product nach den Primidealen $\mathfrak{p}$ des Körpers $k(\zeta)$, aus welchen die Primideale $\mathfrak{P}$ herstammen, so gehört, wie man aus Satz 149 schliesst, zu einem beliebigen Primideal $\mathfrak{p}$ in dem Producte das Glied

$$\frac{1}{(1-n(\mathfrak{p})^{-s})^l} \quad \text{oder} \quad \frac{1}{1-n(\mathfrak{p})^{-s}} \quad \text{oder} \quad \frac{1}{1-n(\mathfrak{p})^{-ls}},$$

je nachdem $\left\{\frac{\alpha}{\mathfrak{p}}\right\} = 1$ oder $= 0$ oder $\neq 1$ und $\neq 0$ ausfällt. Wir schreiben diese drei Ausdrücke in der ihnen gemeinschaftlichen Form

$$\frac{1}{1-n(\mathfrak{p})^{-s}} \prod_{(m)} \frac{1}{1-\left\{\frac{\alpha}{\mathfrak{p}}\right\}^m n(\mathfrak{p})^{-s}} \qquad (m=1, 2, \ldots, l-1)$$

und erhalten so

$$(99.) \quad \zeta_K(s) = \prod_{(\mathfrak{p})} \frac{1}{1-n(\mathfrak{p})^{-s}} \prod_{(\mathfrak{p})} \prod_{(m)} \frac{1}{1-\left\{\frac{\alpha}{\mathfrak{p}}\right\}^m n(\mathfrak{p})^{-s}};$$

darin zeigt das Product $\prod\limits_{(m)}$ an, dass der Exponent m jeden der Werte 1, 2, ..., $l-1$ durchlaufen soll, und es sind die beiden Producte $\prod\limits_{(\mathfrak{p})}$ über alle Primideale $\mathfrak{p}$ in $k(\zeta)$ zu erstrecken. Nun stellt jeder der beiden Ausdrücke

$$\underset{s=1}{L}\,(s-1) \prod_{(\mathfrak{p})} \frac{1}{1-n(\mathfrak{p})^{-s}}, \quad \underset{s=1}{L}\,(s-1)\zeta_K(s)$$

eine endliche und von 0 verschiedene Grösse dar, wie wir erkennen, wenn wir den Satz 56 einmal auf den Kreiskörper $k(\zeta)$ und dann auf den Kummer'schen Körper $K = k(\sqrt[l]{\alpha}, \zeta)$ anwenden. Durch Multipli-

cation der Gleichung (99.) mit $s-1$ und Uebergang zur Grenze für $s=1$ ergiebt sich dann, dass auch der im Hülfssatze 27 angegebene Ausdruck eine endliche und von 0 verschiedene Grösse besitzt.

§ 135.

Primideale des Kreiskörpers $k(\zeta)$ mit vorgeschriebenen Potenzcharakteren.

Satz 152. Es seien $\alpha_1, \ldots, \alpha_t$ irgend t ganze Zahlen des Kreiskörpers $k(\zeta)$, welche die Bedingung erfüllen, dass das Product

$$\alpha_1^{m_1}\alpha_2^{m_2}\ldots\alpha_t^{m_t},$$

wenn man jeden der Exponenten $m_1, m_2, \ldots, m_t$ die Werte 0, 1, 2, ..., $l-1$ durchlaufen lässt, jedoch das eine Wertsystem $m_1=0$, $m_2=0, \ldots, m_t=0$ ausschliesst, dabei niemals die $l$te Potenz einer Zahl in $k(\zeta)$ wird; es seien ferner $\gamma_1, \gamma_2, \ldots, \gamma_t$ nach Belieben vorgeschriebene $l$te Einheitswurzeln: dann giebt es im Kreiskörper $k(\zeta)$ stets unendlich viele Primideale $\mathfrak{p}$, für die jedesmal bei einem gewissen zu l primen Exponenten m

$$\left\{\frac{\alpha_1}{\mathfrak{p}}\right\}^m=\gamma_1,\quad \left\{\frac{\alpha_2}{\mathfrak{p}}\right\}^m=\gamma_2,\quad \ldots,\quad \left\{\frac{\alpha_t}{\mathfrak{p}}\right\}^m=\gamma_t$$

wird. [*Kummer*[20].]

Beweis. Wir haben, so lange $s>1$ ist,

$$(100.)\quad \begin{cases} \log\sum\limits_{(\mathfrak{j})}\dfrac{1}{n(\mathfrak{j})^s}=\sum\limits_{(\mathfrak{p})}\log\dfrac{1}{1-n(\mathfrak{p})^{-s}}=\sum\limits_{(\mathfrak{p})}\dfrac{1}{n(\mathfrak{p})^s}+S, \\ S=\frac{1}{2}\sum\limits_{(\mathfrak{p})}\dfrac{1}{n(\mathfrak{p})^{2s}}+\frac{1}{3}\sum\limits_{(\mathfrak{p})}\dfrac{1}{n(\mathfrak{p})^{3s}}+\cdots, \end{cases}$$

wo $\sum\limits_{(\mathfrak{j})}$ über alle Ideale $\mathfrak{j}$ und $\sum\limits_{(\mathfrak{p})}$ jedesmal über alle Primideale $\mathfrak{p}$ des Körpers $k(\zeta)$ zu erstrecken ist. Da der Ausdruck S, wie in § 50 gezeigt worden ist, für $s=1$ endlich bleibt, so folgt aus (100.), indem die linke Seite für $s=1$ unendlich wird, dass die über alle Primideale $\mathfrak{p}$ des Körpers $k(\zeta)$ erstreckte Summe

$$\sum_{(\mathfrak{p})}\frac{1}{n(\mathfrak{p})^s}$$

bei Annäherung von s an 1 über alle Grenzen wächst. Ist ferner α eine beliebige ganze Zahl in $k(\zeta)$, so gilt ähnlich für $s>1$ stets

$$(101.)\quad \begin{cases} \log \underset{(\mathfrak{p})}{\Pi} \dfrac{1}{1-\left\{\dfrac{\alpha}{\mathfrak{p}}\right\} n(\mathfrak{p})^{-s}} = \underset{(\mathfrak{p})}{\Sigma} \left\{\dfrac{\alpha}{\mathfrak{p}}\right\} \dfrac{1}{n(\mathfrak{p})^s} + S(\alpha), \\ S(\alpha) = \frac{1}{2} \underset{(\mathfrak{p})}{\Sigma} \left\{\dfrac{\alpha}{\mathfrak{p}}\right\}^2 \dfrac{1}{n(\mathfrak{p})^{2s}} + \frac{1}{3} \underset{(\mathfrak{p})}{\Sigma} \left\{\dfrac{\alpha}{\mathfrak{p}}\right\}^3 \dfrac{1}{n(\mathfrak{p})^{3s}} + \cdots, \end{cases}$$

und hier bleibt wiederum $S(\alpha)$ für $s=1$ endlich. Es sei jetzt m eine der Zahlen $1, 2, \ldots, l-1$. Wir setzen in (101.)

$$\alpha = \alpha_*^m = \alpha_1^{mu_1} \alpha_2^{mu_2} \ldots \alpha_t^{mu_t}$$

und multipliciren die entstehende Gleichung noch mit dem Factor $\gamma_1^{-u_1}\gamma_2^{-u_2}\ldots\gamma_t^{-u_t}$; wir erteilen dann jedem der t Exponenten $u_1, u_2, \ldots, u_t$ nach einander alle die l Werte $0, 1, \ldots, l-1$, jedoch so, dass das eine Wertsystem $u_1=0, u_2=0, \ldots, u_t=0$ ausgeschlossen bleibt. Werden die auf diese Weise hervorgehenden l^t-1 Gleichungen sämtlich zu (100.) addirt, so entsteht die Beziehung

$$(102.)\quad \begin{cases} \underset{(\mathfrak{p})}{\Sigma} \dfrac{1}{n(\mathfrak{p})^s} + S + \underset{(u_1,\ldots,u_t)}{\Sigma} \gamma_1^{-u_1}\ldots\gamma_t^{-u_t} \log \underset{(\mathfrak{p})}{\Pi} \dfrac{1}{1-\left\{\dfrac{\alpha_1^{u_1}\ldots\alpha_t^{u_t}}{\mathfrak{p}}\right\}^m n(\mathfrak{p})^{-s}} \\ = \underset{(\mathfrak{p})}{\Sigma} [1][2]\ldots[t] \dfrac{1}{n(\mathfrak{p})^s} + S + \underset{(u_1,\ldots,u_t)}{\Sigma} \gamma_1^{-u_1}\gamma_2^{-u_2}\ldots\gamma_t^{-u_t} S(\alpha_*^m), \end{cases}$$

wo für den Augenblick

$$[1] = 1 + \left(\gamma_1^{-1}\left\{\frac{\alpha_1}{\mathfrak{p}}\right\}^m\right) + \left(\gamma_1^{-1}\left\{\frac{\alpha_1}{\mathfrak{p}}\right\}^m\right)^2 + \cdots + \left(\gamma_1^{-1}\left\{\frac{\alpha_1}{\mathfrak{p}}\right\}^m\right)^{l-1},$$

$$[2] = 1 + \left(\gamma_2^{-1}\left\{\frac{\alpha_2}{\mathfrak{p}}\right\}^m\right) + \left(\gamma_2^{-1}\left\{\frac{\alpha_2}{\mathfrak{p}}\right\}^m\right)^2 + \cdots + \left(\gamma_2^{-1}\left\{\frac{\alpha_2}{\mathfrak{p}}\right\}^m\right)^{l-1},$$

. . . .

$$[t] = 1 + \left(\gamma_t^{-1}\left\{\frac{\alpha_t}{\mathfrak{p}}\right\}^m\right) + \left(\gamma_t^{-1}\left\{\frac{\alpha_t}{\mathfrak{p}}\right\}^m\right)^2 + \cdots + \left(\gamma_t^{-1}\left\{\frac{\alpha_t}{\mathfrak{p}}\right\}^m\right)^{l-1}$$

gesetzt ist; ausserdem ist in $S(\alpha_*^m)$ für α_*^m der oben angegebene Ausdruck einzusetzen. Wenn wir nun in der ersten Summe rechter Hand in (102.) von denjenigen Gliedern absehen — ihr Aggregat möge G_m heissen —, die den in $\alpha_1, \ldots, \alpha_t, \lambda$ aufgehenden Primidealen $\mathfrak{p}$ entsprechen und die nur in endlicher Anzahl vorhanden sind, so hat der übrige unendliche Teil dieser Summe offenbar den Wert $l^t \underset{(\mathfrak{q})}{\Sigma} \dfrac{1}{n(\mathfrak{q})^s}$, wo $\mathfrak{q}$ nur alle diejenigen unter den Primidealen $\mathfrak{p}$ des Körpers $k(\zeta)$ durch-

läuft, für welche die t Bedingungen

$$(103.)\qquad \left\{\frac{\alpha_1}{\mathfrak{p}}\right\}^m = \gamma_1, \quad \ldots, \quad \left\{\frac{\alpha_t}{\mathfrak{p}}\right\}^m = \gamma_t$$

sämtlich erfüllt sind. Bilden wir nun die Gleichungen (102.) nach einander für $m = 1, 2, \ldots, l-1$ und summiren die entstehenden Formeln, so erhalten wir

$$(104.)\quad \begin{cases} '(l-1)\sum\limits_{(\mathfrak{p})} \dfrac{1}{n(\mathfrak{p})^s} + (l-1)S \\ \quad + \sum\limits_{(u_1,\ldots,u_t)} \gamma_1^{-u_1}\cdots\gamma_t^{-u_t} \log \prod\limits_{(\mathfrak{p})}\prod\limits_{(m)} \dfrac{1}{1-\left\{\dfrac{\alpha_1^{u_1}\cdots\alpha_t^{u_t}}{\mathfrak{p}}\right\}^m n(\mathfrak{p})^{-s}} \\ = l^t \sum\limits_{(\mathfrak{r})} \dfrac{1}{n(\mathfrak{r})^s} + \sum\limits_{(m)} G_m + (l-1)S + \sum\limits_{(u_1,\ldots,u_t)} \gamma_1^{-u_1}\cdots\gamma_t^{-u_t} \sum\limits_{(m)} S(\alpha_*^m); \end{cases}$$

hierbei hat in dem ersten Summenausdruck rechter Hand $\mathfrak{r}$ alle Primideale $\mathfrak{p}$ in $k(\zeta)$ zu durchlaufen, welche irgend einem von den $l-1$ Bedingungssystemen genügen, die aus (103.) entstehen, wenn man darin $m = 1, = 2, \ldots, = l-1$ einführt; für $\gamma_1 = 1, \ldots, \gamma_t = 1$ sind diese Bedingungssysteme identisch und die betreffenden Primideale $l-1$ mal zu nehmen. Gehen wir nun zur Grenze für $s = 1$ über, so wird die erste Summe Σ linker Hand in (104.) nach den Ausführungen zu Beginn des Beweises über alle Grenzen wachsen, und die zweite Summe Σ linker Hand bleibt auf Grund von Hülfssatz 27 für $s = 1$ endlich. Da auch die Summen S und $S(\alpha_*^m)$ sämtlich endlich bleiben, so folgt dann, dass der Ausdruck $\Sigma \dfrac{1}{n(\mathfrak{r})^s}$ für $s = 1$ über alle Grenzen wächst, und also sind die betreffenden Primideale $\mathfrak{r}$ in unendlicher Anzahl vorhanden; diese Primideale $\mathfrak{r}$ erfüllen hinsichtlich ihrer Potenzcharaktere genau die Forderungen des Satzes 152.

Capitel XXXI.

Der reguläre Kreiskörper.

§ 136.

Die Definition des regulären Kreiskörpers, der regulären Primzahl und des regulären Kummer'schen Körpers.

Es bedeute l eine ungerade Primzahl und $k(\zeta)$ den durch $\zeta = e^{\frac{2i\pi}{l}}$ bestimmten Kreiskörper: dieser Kreiskörper $k(\zeta)$ heisse ein **regulärer**

Kreiskörper und die Primzahl l **eine reguläre Primzahl,** wenn die Anzahl h der Idealklassen des Körpers $k(\zeta)$ nicht durch l teilbar ist. Die weiteren Capitel werden lediglich von regulären Kreiskörpern und von solchen Kummer'schen Körpern handeln, welche aus regulären Kreiskörpern entspringen, und die ich daher **reguläre Kummer'sche Körper** nennen will; für dieselben können wir sofort folgende einfache Thatsache beweisen:

Satz 153. Es sei $k(\zeta)$ ein regulärer Kreiskörper und K ein aus $k(\zeta)$ entspringender Kummer'scher Körper: wenn dann ein Ideal $\mathfrak{j}$ des Körpers $k(\zeta)$ in dem Körper K Hauptideal ist, so ist das Ideal $\mathfrak{j}$ auch in dem Kreiskörper $k(\zeta)$ selbst ein Hauptideal.

Beweis. Setzen wir $\mathfrak{j} = (A)$, wo A eine ganze Zahl in K bedeutet, so folgt, indem wir die Relativnorm bilden $\mathfrak{j} = (N_k(A))$, d. h. es gilt in $k(\zeta)$ die Aequivalenz $\mathfrak{j}^l \sim 1$. Andererseits ist auch $\mathfrak{j}^h \sim 1$, wobei h die Klassenanzahl von $k(\zeta)$ bedeutet. Bestimmen wir nun zwei ganze rationale positive Zahlen a und b, so dass $al - bh = 1$ wird, so folgt $\mathfrak{j}^{al-bh} \sim 1$, d. h. es ist $\mathfrak{j}$ in $k(\zeta)$ ein Hauptideal.

Es entsteht weiter die Aufgabe, ein Kriterium zu finden, durch welches sich auf leichte Weise ermitteln lässt, ob eine Primzahl l regulär ist. Es sollen zunächst zwei Hülfssätze entwickelt werden, die zu einem solchen Kriterium führen.

§ 137.

Ein Hülfssatz über die Teilbarkeit des ersten Factors der Klassenanzahl von $k\left(e^{\frac{2i\pi}{l}}\right)$ durch l.

Hülfssatz 28. Ist l eine ungerade Primzahl und $k(\zeta)$ der Kreiskörper der $l$ten Einheitswurzeln, so ist der erste Factor der Klassenanzahl von $k(\zeta)$ dann und nur dann durch l teilbar, wenn l im Zähler einer der ersten $l^* = \frac{l-3}{2}$ Bernoulli'schen Zahlen aufgeht. [*Kummer* [8], *Kronecker* [5].]

Beweis. In Satz 142 ist die Klassenanzahl h des Körpers $k(\zeta)$ als Product von zwei Factoren dargestellt; wir betrachten den dort angegebenen Ausdruck für den ersten Factor dieser Klassenanzahl. Zur Abkürzung werde $Z = e^{\frac{2i\pi}{l-1}}$ gesetzt; ferner denken wir uns die zu Grunde gelegte Primitivzahl r nach l speciell derart angenommen, dass

$r^{\frac{l-1}{2}}+1$ nur durch die erste Potenz von l teilbar ist. Es sei endlich, wie in § 108 und § 109, allgemein r_i der kleinste positive Rest von r^i nach l und $q_i = \frac{rr_i - r_{i+1}}{l}$.

Der erste Factor der Klassenanzahl h stellt sich in Satz 142 als ein Bruch dar, dessen Nenner den Werth $(2l)^{l^*}$ hat, und dessen Zähler von der Gestalt

$$(105.) \qquad f(Z)f(Z^3)f(Z^5)\dots f(Z^{l-2})$$

ist, wo zur Abkürzung $f(x)$ die ganzzahlige Function

$$f(x) = r_0 + r_1 x + r_2 x^2 + \dots + r_{l-2} x^{l-2}$$

bezeichnet. Wird ferner

$$g(x) = q_0 + q_1 x + q_2 x^2 + \dots + q_{l-2} x^{l-2}$$

gesetzt, so ergiebt sich leicht

$$(rZ-1)f(Z) = lZ.g(Z),$$

und da infolge der Wahl von r das Product

$$(rZ-1)(rZ^3-1)\dots(rZ^{l-2}-1) = (-1)^{\frac{l-1}{2}}\left(r^{\frac{l-1}{2}}+1\right)$$

genau durch die erste Potenz von l teilbar ist, so folgt, dass der Zähler (105.) des ersten Factors von h nur dann durch $l^{\frac{l-1}{2}} = l^{l^*+1}$ teilbar ist, wenn die Zahl

$$g(Z)g(Z^3)g(Z^5)\dots g(Z^{l-2})$$

durch l teilbar ist. Nun ist $\mathfrak{L} = (l, Z-r)$ ein in l aufgehendes Primideal des Körpers $k(Z)$, und da offenbar $Z \equiv r$ nach $\mathfrak{L}$ ausfällt, so ist

$$g(Z)g(Z^3)\dots g(Z^{l-2}) \equiv g(r)g(r^3)\dots g(r^{l-2}), \quad (\mathfrak{L});$$

folglich ist der erste Factor der Klassenanzahl h nur dann durch l teilbar, wenn mindestens eine der $\frac{l-1}{2}$ Congruenzen

$$g(r^{2t-1}) = q_0 + q_1 r^{2t-1} + q_2 r^{2(2t-1)} + \dots + q_{l-2} r^{(l-2)(2t-1)} \equiv 0, \quad (l)$$
$$\left(t = 1, 2, 3, \dots, \frac{l-1}{2}\right)$$

erfüllt ist.

Es bedeute nun t eine der Zahlen 1, 2, 3, ..., $\frac{l-1}{2}$. Erheben wir dann die Identität

$$rr_i = r_{i+1} + (rr_i - r_{i+1})$$

in die $(2t)$te Potenz und bedenken, dass $rr_i - r_{i+1}$ durch l teilbar ist, so ergiebt sich die Congruenz

$$r^{2t} r_i^{2t} \equiv r_{i+1}^{2t} + 2t(rr_i - r_{i+1}) r_{i+1}^{2t-1}, \quad (l^2)$$

oder

$$2t(rr_i - r_{i+1}) r_{i+1}^{2t-1} \equiv r^{2t} r_i^{2t} - r_{i+1}^{2t}, \quad (l^2)$$

und da offenbar

$$(rr_i - r_{i+1}) r_{i+1}^{2t-1} \equiv (rr_i - r_{i+1}) r^{i(+1)(2t-1)}, \quad (l^2)$$

ist, so folgt

$$2t(rr_i - r_{i+1}) r^{(i+1)(2t-1)} \equiv r^{2t} r_i^{2t} - r_{i+1}^{2t}, \quad (l^2).$$

Diese allgemeine Congruenz ergiebt bei Summation über die Werte $i = 0, 1, 2, \ldots, l-2$

$$2tlr^{2t-1} \sum_{(i)} q_i r^{i(2t-1)} \equiv r^{2t} \sum_{(i)} r_i^{2t} - \sum_{(i)} r_{i+1}^{2t}, \quad (l^2).$$

Da nun

$$\sum_{(i)} r_i^{2t} = \sum_{(i)} r_{i+1}^{2t} = 1^{2t} + 2^{2t} + 3^{2t} + \cdots + (l-1)^{2t}$$

ist, so folgt, dass die Zahl $g(r^{2t-1})$ dann und nur dann durch l teilbar ist, wenn die Zahl

$$(106.) \qquad (r^{2t}-1)(1^{2t} + 2^{2t} + 3^{2t} + \cdots + (l-1)^{2t})$$

durch l^2 teilbar ist. Wegen der über die Primitivzahl r gemachten Annahme ist nun der Ausdruck (106.) für $t = \frac{l-1}{2}$ sicher nicht durch l^2 teilbar. Für $t = 1, 2, \ldots, \frac{l-3}{2}$ gilt auf Grund der Bernoulli'schen Summenformel jedesmal die Congruenz

$$1^{2t} + 2^{2t} + 3^{2t} + \cdots + (l-1)^{2t} \equiv (-1)^{t+1} B_t l, \quad (l^2),$$

wo B_t die $t$te **Bernoulli'sche Zahl** bedeutet, und somit erkennen wir, dass die Teilbarkeit wenigstens einer der Zahlen (106.) für

$$t = 1, 2, \ldots, \frac{l-3}{2}$$

durch l^2 mit der Teilbarkeit wenigstens eines der Zähler der $\frac{l-3}{2}$ ersten Bernoulli'schen Zahlen durch l gleichbedeutend ist. Der Beweis des Hülfssatzes 28 ist dadurch erbracht.

§ 138.

Ein Hülfssatz über die Einheiten des Kreiskörpers $k\left(e^{\frac{2i\pi}{l}}\right)$ für den Fall, dass l in den Zählern der ersten $\frac{l-3}{2}$ Bernoulli'schen Zahlen nicht aufgeht.

Hülfssatz 29. Wenn l eine ungerade Primzahl bedeutet, welche in den Zählern der ersten $l^* = \frac{l-3}{2}$ Bernoulli'schen Zahlen nicht aufgeht, so lässt sich aus den Kreiseinheiten des Körpers $k(\zeta)$ der $l$ten Einheitswurzeln stets durch Bildung geeigneter Producte und Quotienten ein System von solchen l^* Einheiten $\varepsilon_1, \ldots, \varepsilon_{l^*}$ ableiten, für welche l^* Congruenzen von der Gestalt

$$(107.)\qquad \begin{cases} \varepsilon_1 \equiv 1 + a_1\lambda^2, & (\mathfrak{l}^3), \\ \varepsilon_2 \equiv 1 + a_2\lambda^4, & (\mathfrak{l}^5), \\ \varepsilon_3 \equiv 1 + a_3\lambda^6, & (\mathfrak{l}^7), \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot & \\ \varepsilon_{l^*} \equiv 1 + a_{l^*}\lambda^{l-3}, & (\mathfrak{l}^{l-2}) \end{cases}$$

gelten, wo $a_1, a_2, \ldots, a_{l^*}$ ganze rationale, durch l nicht teilbare Zahlen bedeuten; dabei ist $\lambda = 1-\zeta$, $\mathfrak{l} = (\lambda)$ gesetzt. [*Kummer* [12].]

Beweis. Wir gehen aus von der Kreiseinheit (vgl. § 98)

$$(108.)\qquad \varepsilon = \sqrt{\frac{(1-\zeta^r)(1-\zeta^{-r})}{(1-\zeta)(1-\zeta^{-1})}},$$

wo r eine Primitivzahl nach l bezeichnet. Wir setzen dann $\eta = \varepsilon^{l-1}$ und

$$(109.)\qquad \varepsilon_t = \eta^{(r^2-s)(r^4-s)(r^6-s)\ldots(r^{2t-2}-s)(r^{2t+2}-s)(r^{2t+4}-s)\ldots(r^{l-3}-s)}$$

für $t = 1, 2, 3, \ldots, l^*$, wo $s = (\zeta : \zeta^r)$ im Exponenten symbolisch zu verstehen ist.

Die Einheit η ist als $(l-1)$te Potenz einer ganzen Zahl in $k(\zeta)$ notwendig $\equiv 1$ nach $\mathfrak{l}$, und das Gleiche gilt dann auch von jeder der

Einheiten ε_t. Wir denken uns nun allgemein bei jedem Werte t die zur Einheit ε_t gehörende Function $\varepsilon_t(x)$ gemäss § 131 gebildet; dann gelten für die rationalen Zahlen

$$\mathrm{l}^{(1)}(\varepsilon_t), \quad \mathrm{l}^{(2)}(\varepsilon_t), \quad \ldots, \quad \mathrm{l}^{(l-2)}(\varepsilon_t),$$

d. h. für die Werte der ersten $l-2$ Differentialquotienten des Logarithmus von $\varepsilon_t\,(\mathrm{e}^v)$ an der Stelle $v=0$, die Congruenzen:

$$(110.)\quad \begin{cases} \mathrm{l}^{(u)}(\varepsilon_t) \equiv 0, & (l) \\ \quad (u=1,\,2,\,3,\,\ldots,\,2t-1,\,2t+1,\,\ldots,\,l-3,\,l-2), & \\ \mathrm{l}^{(2t)}(\varepsilon_t) \equiv (-1)^{t+l^*} \dfrac{B_t}{4tr^{2t}}, & (l) \\ \quad (t=1,\,2,\,\ldots,\,l^*). & \end{cases}$$

Um dies zu beweisen, bedenken wir, dass nach der ersten Formel S. 413 oben bei der Berechnung der ersten $l-2$ Differentialquotienten

$$\mathrm{l}^{(1)}(\eta), \quad \mathrm{l}^{(2)}(\eta), \quad \ldots, \quad \mathrm{l}^{(l-2)}(\eta)$$

in Bezug auf die Zahl η an Stelle der zu η gehörenden Function direct die folgende ganze Function

$$\tilde{\eta}(x) = \left(\frac{(1-x^r)(1-x^{-r})}{(1-x)(1-x^{-1})}\right)^{\frac{l-1}{2}}$$

genommen werden darf. Nun gilt bekanntlich die Entwickelung

$$\log\frac{\mathrm{e}^v-1}{v} = +\frac{1}{2}v + \frac{B_1}{2.2!}v^2 - \frac{B_2}{4.4!}v^4 + \frac{B_3}{6.6!}v^6 - \cdots,$$

wo B_1, B_2, B_3, ... die Bernoulli'schen Zahlen bedeuten. Mit Benutzung dieser unendlichen Reihe folgt

$$(111.)\quad \begin{cases} \log\tilde{\eta}(\mathrm{e}^v) = (l-1)\Big\{\log r + (r^2-1)\dfrac{B_1}{2.2!}v^2 \\ \qquad\qquad - (r^4-1)\dfrac{B_2}{4.4!}v^4 + (r^6-1)\dfrac{B_3}{6.6!}v^6 - \cdots\Big\}. \end{cases}$$

Von derselben Verwendbarkeit wie $\tilde{\eta}(\mathrm{e}^v)$ in Bezug auf die Zahl η ist die Function $\tilde{\eta}(\mathrm{e}^{rv})$ in Bezug auf die Zahl $s\eta$, $\tilde{\eta}(\mathrm{e}^{r^2v})$ in Bezug auf $s^2\eta$ u. s. f. Ersetzen wir dann nach Entwickelung des Ausdrucks (109.) von ε_t darin η, $s\eta$, $s^2\eta$, ... durch $\tilde{\eta}(\mathrm{e}^v)$, $\tilde{\eta}(\mathrm{e}^{rv})$, $\tilde{\eta}(\mathrm{e}^{r^2v})$, ..., so entsteht eine Function $\tilde{\varepsilon}_t(\mathrm{e}^v)$, welche nach den Ausführungen auf S. 413 bei Bildung von $\mathrm{l}^{(1)}(\varepsilon_t)$, $\mathrm{l}^{(2)}(\varepsilon_t)$, ..., $\mathrm{l}^{(l-2)}(\varepsilon_t)$ die Stelle der Function

$\varepsilon_t(\mathrm{e}^v)$ vertreten kann. Aus (111.) ergiebt sich:

$$\log \tilde{\varepsilon}_t(\mathrm{e}^v) = (l-1)\Big\{C + (-1)^t (r^2 - r^{2t})(r^4 - r^{2t}) \ldots$$

$$\ldots (r^{2t-2} - r^{2t})(r^{2t+2} - r^{2t})(r^{2t+4} - r^{2t}) \ldots (r^{l-3} - r^{2t})(1 - r^{2t}) \frac{B_t}{2t(2t)!} v^{2t}\Big\}$$

$$+ C_{l-1} v^{l-1} + C_{l+1} v^{l+1} + \cdots,$$

wo C, C_{l-1}, C_{l+1}, ... gewisse Constanten bedeuten. Das ausführlich geschriebene Product in dem Coefficienten von v^{2t} ist

$$(-1)^{l^*} \left[\frac{\mathrm{d}(x-1)(x-r^2)\ldots(x-r^{l-3})}{\mathrm{d}x}\right]_{(x=r^{2t})},$$

und die hier zu differentiirende Function ist $\equiv x^{\frac{l-1}{2}} - 1$ nach l. Aus dieser Entwickelung folgt nun unmittelbar die Richtigkeit der Congruenzen (110.).

Da nach Voraussetzung die Zähler der ersten l^* Bernoulli'schen Zahlen $B_1, \ldots, B_{l^*}$ nicht durch l teilbar sein sollen, so sind nach (110.) die l^* Differentialquotienten $\mathrm{l}^{(2t)}(\varepsilon_t)$ für $t = 1, 2, \ldots, l^*$ sämtlich der Null incongruent nach l. Aus dem letzteren Umstande schliessen wir zunächst, dass keine der Einheiten $\varepsilon_1, \ldots, \varepsilon_{l^*}$ nach l der Zahl 1 congruent ausfällt. Setzen wir daher

$$(112.) \qquad \begin{cases} \varepsilon_1 \equiv 1 + a_1 \lambda^{e_1}, & (\mathfrak{l}^{e_1+1}), \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot & \\ \varepsilon_{l^*} \equiv 1 + a_{l^*} \lambda^{e_{l^*}}, & (\mathfrak{l}^{e_{l^*}+1}) \end{cases}$$

mit solchen Exponenten $e_1, \ldots, e_{l^*}$, dass dabei $a_1, \ldots, a_{l^*}$ ganze rationale, nicht durch l teilbare Zahlen bedeuten, so sind diese Exponenten $e_1, \ldots, e_{l^*}$ sämtlich $< l-1$. Nun erhält man aus den Congruenzen (112.), da die Entwickelung eines Ausdruckes $(1-\mathrm{e}^v)^g$ nach Potenzen von v mit dem Gliede $(-1)^g v^g$ beginnt, für die Einheit ε_t die Congruenzen

$$\mathrm{l}^{(1)}(\varepsilon_t) \equiv 0, \quad \mathrm{l}^{(2)}(\varepsilon_t) \equiv 0, \quad \ldots, \quad \mathrm{l}^{(e_t-1)}(\varepsilon_t) \equiv 0, \quad (l),$$

$$\mathrm{l}^{(e_t)}(\varepsilon_t) \equiv (-1)^{e_t} a_t \cdot e_t!, \qquad (l),$$

und da a_t nicht durch l teilbar sein soll, so ergiebt sich mit Rücksicht auf die vorhin bemerkte Folgerung aus den Congruenzen (110.) $e_t = 2t$, womit der Hülfssatz 29 bewiesen ist.

§ 139.

Ein Kriterium für die regulären Primzahlen.

Der folgende Satz liefert ein einfaches Kriterium für die regulären Primzahlen l:

Satz 154. Eine ungerade Primzahl l ist dann und nur dann regulär, wenn sie in den Zählern der ersten $l^* = \frac{l-3}{2}$ Bernoulli'schen Zahlen nicht aufgeht. [*Kummer*[8].]

Beweis. Der Hülfssatz 28 zeigt, dass, wenn l im Zähler wenigstens einer der ersten l^* Bernoulli'schen Zahlen aufgeht, die Klassenanzahl h des Körpers $k(\zeta)$ jedenfalls durch l teilbar ist. Sind hingegen die Zähler der ersten l^* Bernoulli'schen Zahlen sämtlich zu l prim, so zeigt der nämliche Hülfssatz 28, dass der erste Factor der Klassenanzahl zu l prim ist. Es bedarf also nur noch des Nachweises, dass auch der zweite Factor der Klassenanzahl h nicht durch l teilbar ist, wenn die Zähler der ersten l^* Bernoulli'schen Zahlen sämtlich zu l prim sind. Diesen Nachweis führen wir in folgender Weise:

Es sei $\gamma_1, \ldots, \gamma_{l^*}$ ein System von reellen l^* Grundeinheiten des Körpers $k(\zeta)$, wie ein solches nach Satz 127 stets existirt; dann können wir setzen:

$$(113.)\qquad s^t\varepsilon = \gamma_1^{m_{1t}}\gamma_2^{m_{2t}}\cdots\gamma_{l^*}^{m_{l^*t}}$$

für $t = 0, 1, 2, \ldots, l^*-1$, wo die Exponenten $m_{1t}, m_{2t}, \ldots, m_{l^*t}$ ganze rationale Zahlen sind und ε die in Formel (108.) definirte Kreiseinheit bedeutet. Aus (113.) erhalten wir:

$$(114.)\qquad \log|s^t\varepsilon| = m_{1t}\log|\gamma_1| + m_{2t}\log|\gamma_2| + \cdots + m_{l^*t}\log|\gamma_{l^*}|$$

für $t = 0, 1, 2, \ldots, l^*-1$, wo unter den Logarithmen deren reelle Werte verstanden werden sollen. Andererseits bringen die Definitionsgleichungen (109.) der Einheiten $\varepsilon_1, \ldots, \varepsilon_{l^*}$ ein Gleichungssystem von der Gestalt

$$(115.)\qquad \varepsilon_t = \varepsilon^{n_{1t}}(s\varepsilon)^{n_{2t}}\cdots(s^{l^*-1}\varepsilon)^{n_{l^*t}} \qquad (t = 1, 2, \ldots, l^*)$$

mit sich. Von demselben gehen wir zu den Gleichungen

$$(116.)\qquad \log\varepsilon_t = n_{1t}\log|\varepsilon| + n_{2t}\log|s\varepsilon| + \cdots + n_{l^*t}\log|s^{l^*-1}\varepsilon| \qquad (t = 1, 2, \ldots, l^*)$$

über, wo für die Logarithmen wieder die reellen Werte eintreten sollen, und vermöge (114.) wird hieraus

$$(117.)\qquad \log\varepsilon_t = M_{1t}\log|\gamma_1| + M_{2t}\log|\gamma_2| + \cdots + M_{l^*t}\log|\gamma_{l^*}|, \qquad (t=1,2,\ldots,l^*)$$

wo $M_{1t}, M_{2t}, \ldots, M_{l^*t}$ die bekannten bilinearen Verbindungen der $2l^{*2}$ ganzen rationalen Zahlen $n_{11}, n_{21}, \ldots, n_{l^*, l^*}$; $m_{10}, m_{20}, \ldots \ldots, m_{l^*, l^*-1}$ bedeuten. Aus den Gleichungssystemen (113.) und (115.) entspringen jedesmal l^*-1 weitere Gleichungssysteme, wenn wir auf die darin vorkommenden Einheiten die Substitutionen $s, s^2, \ldots, s^{l^*-1}$ anwenden. Indem wir dann wieder die betreffenden Logarithmen nehmen, erhalten wir diejenigen Gleichungssysteme, die aus den Gleichungssystemen (114.), (116.) und (117.) hervorgehen, wenn man auf die darin vorkommenden Einheiten der Reihe nach durchgehends die Substitution s, bez. $s^2, \ldots$, bez. s^{l^*-1} anwendet.

Setzen wir nun

$$R = \begin{vmatrix} \log|\gamma_1|, & \ldots, & \log|\gamma_{l^*}| \\ \log|s\gamma_1|, & \ldots, & \log|s\gamma_{l^*}| \\ \cdot & \cdot & \cdot \\ \log|s^{l^*-1}\gamma_1|, & \ldots, & \log|s^{l^*-1}\gamma_{l^*}| \end{vmatrix},$$

$$\varDelta = \begin{vmatrix} \log|\varepsilon|, & \log|s\varepsilon| & \ldots, & \log|s^{l^*-1}\varepsilon| \\ \log|s\varepsilon|, & \log|s^2\varepsilon|, & \ldots, & \log|s^{l^*}\varepsilon| \\ \cdot & \cdot & \cdot & \cdot \\ \log|s^{l^*-1}\varepsilon|, & \log s^{l^*}|\varepsilon|, & \ldots, & \log|s^{2l^*-2}\varepsilon| \end{vmatrix},$$

$$\bar{\varDelta} = \begin{vmatrix} \log\varepsilon_1, & \log\varepsilon_2, & \ldots, & \log\varepsilon_{l^*} \\ \log s\varepsilon_1, & \log s\varepsilon_2, & \ldots, & \log s\varepsilon_{l^*} \\ \cdot & \cdot & \cdot & \cdot \\ \log s^{l^*-1}\varepsilon_1, & \log s^{l^*-1}\varepsilon_2, & \ldots, & \log s^{l^*-1}\varepsilon_{l^*} \end{vmatrix},$$

so ergiebt eine Anwendung des Multiplicationssatzes der Determinanten

$$(118.)\quad \left\{ \frac{\bar{\varDelta}}{R} = \frac{\bar{\varDelta}}{\varDelta}\cdot\frac{\varDelta}{R} = \begin{vmatrix} M_{11}, & M_{21}, & \ldots, & M_{l^*1} \\ M_{12}, & M_{22}, & \ldots, & M_{l^*2} \\ \cdot & \cdot & \cdot & \cdot \\ M_{1l}, & M_{2l^*}, & \ldots, & M_{l^*l^*} \end{vmatrix} \right..$$

Die rechts stehende Determinante ist eine ganze rationale und überdies eine zu l prime Zahl. Wäre nämlich diese Determinante durch l teil-

bar, so würde man im Stande sein, l^* ganze rationale Zahlen $N_1, \ldots, N_{l^*}$ zu finden, die nicht sämtlich durch l teilbar sind, während die aus ihnen gebildeten Ausdrücke

$$\sum_{(t)} N_t M_{1t}, \quad \sum_{(t)} N_t M_{2t}, \quad \ldots, \quad \sum_{(t)} N_t M_{l^*t}$$
$$(t = 1, 2, \ldots, l^*)$$

sämtlich durch l teilbar ausfallen. Durch Berücksichtigung dieses zweiten Umstandes ergiebt sich aus (117.) eine Gleichung von der Gestalt

$$N_1 \log \varepsilon_1 + N_2 \log \varepsilon_2 + \cdots + N_{l^*} \log \varepsilon_{l^*} = l \log \boldsymbol{E},$$

in welcher $\boldsymbol{E}$ eine gewisse positive Einheit des Körpers $k(\zeta)$ bezeichnet. Setzen wir beide Seiten in den Exponenten von e, so haben wir

$$(119.) \qquad \varepsilon_1^{N_1} \varepsilon_2^{N_2} \ldots \varepsilon_{l_*}^{N_{l^*}} = \boldsymbol{E}^l.$$

Es ist nun das Bestehen einer solchen Gleichung (119.) unmöglich. Denn es würde zunächst $\boldsymbol{E} \equiv \boldsymbol{E}^l \equiv 1$ nach $\mathfrak{l}$ folgen; denken wir uns die zu $\boldsymbol{E}$ gehörende Function $\boldsymbol{E}(x)$ eingeführt und betrachten wir die Werte der ersten $l-2$ Differentialquotienten von $\log \boldsymbol{E}(\mathrm{e}^v)$ an der Stelle $v = 0$, so würden aus (119.) unter Verwendung von (110.) die Congruenzen

$$(-1)^{t+l^*} \frac{B_t}{4 t r^{2t}} N_t \equiv 0, \quad (l), \quad (t = 1, 2, \ldots, l^*)$$

folgen. Es sollen aber die Bernoulli'schen Zahlen $B_1, B_2, \ldots, B_{l^*}$ sämtlich zu l prim und andererseits die Zahlen $N_1, \ldots, N_{l^*}$ nicht sämtlich congruent 0 nach l sein; wir erhalten damit einen Widerspruch.

Hiernach ist die Determinante rechts in (118.) nicht durch l teilbar. Da andererseits ihre Factoren $\frac{\bar{\Delta}}{\Delta}$ und $\frac{\Delta}{R}$ beide ebenfalls als ganze Zahlen erscheinen und $\frac{\Delta}{R}$ den zweiten Factor der Klassenanzahl h darstellt, so ist auch der zweite Factor der Klassenanzahl nicht durch l teilbar. Damit ist der Beweis des Satzes 154 vollständig erbracht.

Auf Grund des Satzes 154 findet sich aus den Werten der ersten 47 Bernoulli'schen Zahlen, dass ausser den drei Primzahlen 37, 59, 67 die unterhalb 100 liegenden Primzahlen sämtlich regulär sind. Wie sich ferner durch Rechnung findet, sind die Klassenanzahlen h der Kreiskörper $k\left(\mathrm{e}^{\frac{2i\pi}{l}}\right)$ für $l = 37, 59, 67$ nur durch die erste und nicht durch eine höhere Potenz von l teilbar. [*Kummer*[11, 26].]

§ 140.

Ein besonderes System von unabhängigen Einheiten im regulären Kreiskörper.

Wir haben in § 139 die Mittel zur Aufstellung eines Systems von Einheiten des regulären Kreiskörpers gewonnen, welches für die weiteren Entwickelungen von Nutzen sein wird.

Satz 155. Ist l eine reguläre Primzahl, so giebt es im Kreiskörper der $l$ten Einheitswurzeln stets ein System von $l^* = \frac{l-3}{2}$ unabhängigen Einheiten $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{l^*}$ von der Art, dass für dieselben die Congruenzen

$$\bar{\varepsilon}_1 \equiv 1+\lambda^2, \quad (\mathfrak{l}^3),$$

$$\bar{\varepsilon}_2 \equiv 1+\lambda^4, \quad (\mathfrak{l}^5),$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

$$\bar{\varepsilon}_{l^*} \equiv 1+\lambda^{l-3}, \quad (\mathfrak{l}^{l-2})$$

erfüllt sind; dabei ist $\lambda = 1-\zeta$, $\mathfrak{l} = (\lambda)$ gesetzt.

Beweis. Da der Kreiskörper $k(\zeta)$ regulär sein soll, so sind in Anbetracht von Satz 154 die Zähler der ersten l^* Bernoulli'schen Zahlen sämtlich zu l prim, und folglich giebt es nach Hülfssatz 29. l^* Einheiten $\varepsilon_1, \ldots, \varepsilon_{l^*}$, welche die in (107.) ausgedrückten Congruenzeigenschaften besitzen. Da dort die Coefficienten $a_1, \ldots, a_{l^*}$ sämtlich zu l prim sind, so können wir l^* ganze rationale Zahlen $b_1, \ldots, b_{l^*}$ bestimmen derart, dass

$$a_1 b_1 \equiv 1, \quad \ldots, \quad a_{l^*} b_{l^*} \equiv 1, \quad (l)$$

wird. Setzen wir dann

$$\bar{\varepsilon}_1 = \varepsilon_1^{b_1}, \quad \ldots, \quad \bar{\varepsilon}_{l^*} = \varepsilon_{l^*}^{b_{l^*}},$$

so erfüllen diese Einheiten $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{l^*}$ jedenfalls die in Satz 155 geforderten Congruenzbedingungen.

Ferner bilden $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}$ ein System von einander unabhängiger Einheiten, weil die in § 138 bestimmten Einheiten $\varepsilon_1, \ldots, \varepsilon_{l^*}$ ein solches waren. Um letzteres einzusehen, nehmen wir im Gegenteil an, dass eine

Gleichung von der Gestalt

$$(120.)\qquad \varepsilon_1^{e_1}\dots\varepsilon_{l^*}^{e_{l^*}} = 1$$

bestehe, wo die Exponenten $e_1, \dots, e_{l^*}$ ganze rationale, nicht sämtlich verschwindende Zahlen sind; dann können wir weiter die Annahme machen, dass diese Exponenten $e_1, \dots, e_{l^*}$ nicht sämtlich durch l teilbar seien, da im engegengesetzten Falle offenbar sofort

$$\varepsilon_1^{\frac{e_1}{l}}\dots\varepsilon_{l^*}^{\frac{e_{l^*}}{l}} = 1$$

folgen würde. Unter der Annahme, dass in (120.) die Exponenten $e_1, \dots, e_{l^*}$ nicht sämtlich durch l teilbar sind, ist aber (120.) von der Gestalt der Gleichung (119.), und dass eine solche Gleichung unmöglich ist, haben wir bereits in § 139 erkannt.

§ 141.

Eine charakteristische Eigenschaft für die Einheiten eines regulären Kreiskörpers.

Satz 156. Wenn l eine reguläre Primzahl bedeutet und im Körper $k(\zeta)$ der $l$ten Einheitswurzeln eine solche Einheit $\boldsymbol{E}$ vorliegt, welche einer ganzen rationalen Zahl nach l congruent ist, so ist sie notwendig die $l$te Potenz einer Einheit dieses Kreiskörpers. [*Kummer* [8].]

Beweis. Wir denken uns ein System von Einheiten $\bar{\varepsilon}_1, \dots, \bar{\varepsilon}_{l^*}$ gemäss Satz 155 bestimmt; da dieselben ein System unabhängiger Einheiten bilden, so giebt es ganze rationale, nicht sämtlich verschwindende Exponenten $e, e_1, \dots, e_{l^*}$, so dass

$$(121.)\qquad \boldsymbol{E}^e = \bar{\varepsilon}_1^{e_1}\dots\bar{\varepsilon}_{l^*}^{e_{l^*}}$$

wird, und wir können, wie sich sofort zeigt, noch annehmen, dass $e, e_1, \dots, e_{l^*}$ nicht sämtlich durch l teilbar sind. Wäre dann e durch l teilbar, so hätte die Gleichung (121.) die Gestalt (119.), und dass eine Gleichung von dieser Gestalt nicht statthaben kann, haben wir bereits erkannt. Wäre andererseits e nicht durch l teilbar, so würde jedenfalls $\boldsymbol{E}^e \equiv 1$ nach $\mathfrak{l}$ und also $\equiv 1$ nach l sein; wir bilden dann für beide Seiten der Gleichung (121.) die logarithmischen Differentialquotienten der zu ihnen gehörenden Functionen. Da wegen $\boldsymbol{E}^e \equiv 1$ nach l die Zahlen $1^{(g)}(\boldsymbol{E}^e)$ für $g < l-1$ sämtlich congruent 0 nach l sind, so folgt, wenn wir dies insbesondere für $g = 2, 4, \dots, 2l^*$ in An-

wendung bringen und die Werte der Zahlen $\mathfrak{l}^{(g)}(\bar{\varepsilon}_1), \ldots, \mathfrak{l}^{(g)}(\bar{\varepsilon}_{l^*})$ in Rücksicht auf (110.) einsetzen, der Reihe nach $e_1 \equiv 0, \ldots, e_{l^*} \equiv 0$ nach l; es wird dann also $\boldsymbol{E}^e = \boldsymbol{H}^l$, wo $\boldsymbol{H}$ eine gewisse Einheit des Kreiskörpers bedeutet, während e nach Voraussetzung eine nicht durch l teilbare ganze rationale Zahl ist. Bestimmen wir nun zwei ganze rationale Zahlen a und b, so dass $ae + bl = 1$ wird, so folgt

$$\boldsymbol{E} = (\boldsymbol{H}^a \boldsymbol{E}^b)^l,$$

und hiermit ist der Beweis des Satzes 156 vollständig erbracht.

Ein wesentlich hiervon verschiedener Beweis des Satzes 156 beruht auf folgender Ueberlegung. Wäre $\boldsymbol{E}$ nicht die $l$te Potenz einer Einheit in $k(\zeta)$, so könnte auch die Einheit $\boldsymbol{H} = \boldsymbol{E}^{1-s}$ nicht die $l$te Potenz einer Einheit sein, wie leicht aus dem Umstande ersichtlich ist, dass $1-s$ und $1+s+\cdots+s^{l-2}$ zwei ganzzahlige Functionen von s sind, die im Sinne der Congruenz nach l keinen gemeinsamen Factor haben. Nun wird aber, wenn wir $\boldsymbol{E}$ congruent einer ganzen rationalen Zahl nach l annehmen, $\boldsymbol{H} \equiv 1$ nach $\mathfrak{l}^l$, und hieraus würde nach dem zweiten Teile von Satz 148 folgen, dass der Kummer'sche Körper $k(\sqrt[l]{\boldsymbol{H}}, \zeta)$ die Relativdiscriminante 1 in Bezug auf $k(\zeta)$ besitzt. Da ferner dieser Kummer'sche Körper relativ-Abel'sch vom Relativgrade l in Bezug auf $k(\zeta)$ ist, so würde endlich aus Satz 94 folgen, dass die Anzahl der Idealklassen des Kreiskörpers $k(\zeta)$ durch l teilbar sein müsste, was der Annahme, dass $k(\zeta)$ ein regulärer Kreiskörper ist, widerspräche.

§ 142.

Der Begriff der primären Zahl im regulären Kreiskörper.

Eine ganze Zahl α des regulären Kreiskörpers $k(\zeta)$ heisst **primär,** wenn sie e r s t e n s semiprimär ist (s. S. 368), und wenn sie z w e i t e n s die Eigenschaft besitzt, dass ihr Product mit der conjugirt imaginären Zahl, also mit $s^{\frac{l-1}{2}}\alpha$, einer ganzen rationalen Zahl nach $l = \mathfrak{l}^{l-1}$ congruent wird. Eine primäre Zahl ist also stets zu $\mathfrak{l}$ prim und hat die Congruenzen

$$\alpha \equiv a, \quad (\mathfrak{l}^2),$$

$$\alpha . s^{\frac{l-1}{2}} \alpha \equiv b, \quad (\mathfrak{l}^{l-1})$$

so zu erfüllen, dass a und b ganze rationale Zahlen sind. [*Kummer*[12].] Es gilt die Thatsache:

Satz 157. In einem regulären Kreiskörper $k(\zeta)$ kann eine beliebige zu $\mathfrak{l}$ prime ganze Zahl α stets durch Multiplication mit einer Einheit in eine primäre Zahl verwandelt werden. [*Kummer*[12].]

Beweis. Bilden wir aus α die Zahl $\beta = \alpha . s^{\frac{l-1}{2}} \alpha$, so ist dieselbe offenbar eine Zahl in dem Unterkörper vom Grade $\frac{l-1}{2}$ des Körpers $k(\zeta)$ und genügt daher einer Congruenz $\beta \equiv a$ nach $\mathfrak{l}^2$, wo a eine ganze rationale, nicht durch l teilbare Zahl bedeutet. Es seien $\bar{\varepsilon}_1, \bar{\varepsilon}_2, \ldots, \bar{\varepsilon}_{l^*}$ die l^* in § 140 bestimmten Einheiten. Ist nun etwa $\beta \equiv a + a_1 \lambda^2$ nach $\mathfrak{l}^4$, wo a_1 eine ganze rationale Zahl bedeute, so bestimme man eine ganze rationale Zahl u_1 so, dass $2au_1 + a_1 \equiv 0$ nach l wird; dann ist notwendig

$$\beta \bar{\varepsilon}_1^{2u_1} \equiv a, \quad (\mathfrak{l}^4).$$

Ist ferner etwa $\beta \bar{\varepsilon}_1^{2u_1} \equiv a + a_2 \lambda^4$ nach $\mathfrak{l}^6$, wo a_2 wieder eine ganze rationale Zahl bedeute, so bestimme man eine ganze rationale Zahl u_2 derart, dass $2au_2 + a_2 \equiv 0$ nach l wird; dann ist

$$\beta \bar{\varepsilon}_1^{2u_1} \bar{\varepsilon}_2^{2u_2} \equiv a, \quad (\mathfrak{l}^6).$$

Fahren wir in der begonnenen Weise fort und setzen am Ende

$$\bar{\varepsilon} = \bar{\varepsilon}_1^{u_1} \bar{\varepsilon}_2^{u_2} \ldots \bar{\varepsilon}_{l^*}^{u_{l^*}},$$

so wird $\beta \bar{\varepsilon}^2 \equiv a$ nach $\mathfrak{l}^{l-1}$. Ist andererseits ζ^* eine solche Potenz von ζ, dass $\zeta^* \alpha$ semiprimär wird, so ist offenbar $\zeta^* \bar{\varepsilon} \alpha$ eine primäre Zahl.

Eine reelle primäre Zahl ist stets einer ganzen rationalen Zahl nach $l = \mathfrak{l}^{l-1}$ congruent. Aus Satz 156 folgt leicht, dass eine primäre Einheit in $k(\zeta)$ stets die $l$te Potenz einer Einheit in $k(\zeta)$ ist.

Wir erörtern noch kurz einen Hülfssatz über primäre Zahlen, welcher uns später von Nutzen sein wird.

Hülfssatz 30. Wenn ν, μ zwei primäre Zahlen des regulären Kreiskörpers $k(\zeta)$ sind, so ist stets

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = 1.$$

Beweis. Wir dürfen annehmen, dass die Zahlen ν, μ beide $\equiv 1$ nach $\mathfrak{l}$ ausfallen, da sonst ihre $(l-1)$ten Potenzen sicher dieser Be-

dingung genügen und wir mit Rücksicht auf $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu^{l-1}, \mu^{l-1}}{\mathfrak{l}}\right\}$ (vgl. S. 414) diese an Stelle der Zahlen ν, μ selbst betrachten können. Nach (83.) ist

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}\left\{\frac{\nu, s^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu, \mu . s^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right\},$$

und da bei unserer Annahme $\mu . s^{\frac{l-1}{2}}\mu \equiv 1$ nach $\mathfrak{l}^{l-1}$ und $\nu \equiv 1$ nach $\mathfrak{l}^2$ ausfällt, so folgt aus der allgemeinen Definition (82.) des Symbols $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ in § 131 unmittelbar $\left\{\frac{\nu, \mu . s^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right\} = 1$, und daher wird

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}\left\{\frac{\nu, s^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right\} = 1.$$

Entsprechend beweisen wir, dass

$$\left\{\frac{\nu, s^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right\}\left\{\frac{s^{\frac{l-1}{2}}\nu, s^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right\} = 1$$

ist. Aus Formel (84.) ergiebt sich ferner:

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}\left\{\frac{s^{\frac{l-1}{2}}\nu, s^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right\} = 1.$$

Die drei letzten Gleichungen zusammengenommen liefern:

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}^2 = 1, \quad \text{d. h.} \quad \left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = 1,$$

und damit ist der Hülfssatz 30 bewiesen.

Capitel XXXII.

Die ambigen Idealklassen und die Geschlechter im regulären Kummer'schen Körper.

§ 143.

Der Begriff der Einheitenschar im regulären Kreiskörper.

Es sei l eine reguläre ungerade Primzahl, und in dem durch $\zeta = e^{\frac{2i\pi}{l}}$ bestimmten regulären Kreiskörper $k(\zeta)$ sei ein solches System E von

Einheiten vorgelegt, in welchem die $l$ten Potenzen aller Einheiten des Körpers $k(\zeta)$ enthalten sind, und welchem überdies die Eigenschaft zukommt, dass das Product und der Quotient von irgend zwei Einheiten des Systems stets wieder dem Systeme angehört. Ein solches System E nenne ich eine **Einheitenschar des Kreiskörpers** $k(\zeta)$. Man kann in einer jeden Einheitenschar E stets eine gewisse Anzahl m von Einheiten $\varepsilon_1, \ldots, \varepsilon_m$ bestimmen von der Art, dass man jede Einheit der Einheitenschar und jede nur einmal erhält, wenn man in dem Ausdruck

$$\varepsilon_1^{u_1}\varepsilon_2^{u_2}\ldots\varepsilon_m^{u_m}\xi^l$$

einem jeden der Exponenten $u_1, \ldots, u_m$ unabhängig von den übrigen alle Werte $0, 1, \ldots, l-1$ erteilt und für ξ eine jede Einheit in $k(\zeta)$ einsetzt. Ein System von Einheiten $\varepsilon_1, \ldots, \varepsilon_m$ dieser Beschaffenheit nenne ich eine **Basis der Einheitenschar** E. Es ist klar, dass für die Einheiten $\varepsilon_1, \ldots, \varepsilon_m$ einer Basis von E niemals eine Relation von der Gestalt

$$\varepsilon_1^{e_1}\ldots\varepsilon_m^{e_m} = \varepsilon^l$$

stattfinden kann, wo $e_1, \ldots, e_m$ ganze rationale, nicht sämtlich durch l teilbare Exponenten sind und ε eine Einheit in $k(\zeta)$ bedeutet. Es lässt sich leicht zeigen, dass für eine jede andere Basis der Einheitenschar E die Anzahl m der Einheiten, aus denen sie besteht, die gleiche sein muss. Diese Zahl m ist daher für die Einheitenschar E eine vollkommen bestimmte; sie heisse der **Grad der Einheitenschar.**

Enthält insbesondere eine Einheitenschar nur die $l$ten Potenzen der Einheiten in $k(\zeta)$, so ist sie die möglichst wenig Einheiten umfassende Einheitenschar, und ihr Grad 0. Ferner bildet die Gesamtheit aller Einheiten des Körpers $k(\zeta)$ eine Einheitenschar; aus dem Umstande, dass nach Satz 127 jede Einheit in $k(\zeta)$ das Product einer $l$ten Einheitswurzel und einer reellen Einheit ist, und aus den Entwickelungen beim Beweise des Satzes 157 entnehmen wir sofort, dass die in § 140 mit $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{\frac{l-3}{2}}$ bezeichneten Einheiten mit der Einheitswurzel ζ zusammen eine Basis dieser umfassendsten Einheitenschar sind. Die aus allen Einheiten des Körpers $k(\zeta)$ bestehende Einheitenschar besitzt folglich den Grad $m = \frac{l-1}{2}$; sie ist offenbar die einzige Einheitenschar vom Grade

$\frac{l-1}{2}$, und es kann überhaupt keine Einheitenschar von höherem als dem $\frac{l-1}{2}$ten Grade geben.

Wie man ferner leicht erkennt, bilden die Relativnormen aller Einheiten eines aus $k(\zeta)$ entspringenden Kummer'schen Körpers $k(\sqrt[l]{\mu}, \zeta)$ für den Kreiskörper $k(\zeta)$ eine Einheitenschar; endlich ist auch die Gesamtheit aller derjenigen Einheiten in $k(\zeta)$ eine Einheitenschar, welche gleich Relativnormen, sei es von Einheiten, sei es von gebrochenen Zahlen des Kummer'schen Körpers $k(\sqrt[l]{\mu}, \zeta)$ sind.

§ 144.

Die ambigen Ideale und die ambigen Idealklassen eines regulären Kummer'schen Körpers.

Es sei $k(\zeta)$ ein regulärer Kreiskörper, und μ eine ganze Zahl in $k(\zeta)$, welche nicht gleich der $l$ten Potenz einer Zahl in $k(\zeta)$ ist; der durch $M = \sqrt[l]{\mu}$ und ζ bestimmte reguläre Kummer'sche Körper $k(M, \zeta)$ werde mit K bezeichnet. Wir suchen nunmehr die Theorie dieses Körpers mittelst der entsprechenden Begriffe und Methoden zu fördern, wie sie in den Capiteln XVII—XVIII in der Theorie des quadratischen Körpers angewandt worden sind.

Die Relativgruppe von K in Bezug auf $k(\zeta)$ wird durch die Potenzen der Substitution $S = (M : \zeta M)$ gebildet; es werde gemäss § 57 ein Ideal $\mathfrak{A}$ des Körpers K ein **ambiges Ideal** genannt, wenn $\mathfrak{A}$ bei Anwendung der Operation S ungeändert bleibt, d. h. $S\mathfrak{A} = \mathfrak{A}$ ist, und wenn ausserdem $\mathfrak{A}$ kein von 1 verschiedenes Ideal des Körpers $k(\zeta)$ als Factor enthält. Nach Satz 93 sind die t in der Relativdiscriminante von K aufgehenden Primideale sämtlich ambig, und es giebt ausser diesen auch keine anderen ambigen Primideale. Ist sodann $\mathfrak{A}$ ein beliebiges ambiges Ideal in K, so schliessen wir aus $\mathfrak{A} = S\mathfrak{A}$ leicht (vgl. § 73), dass auch jedes in $\mathfrak{A}$ aufgehende Primideal des Körpers K ambig sein muss, und daraus folgt dann, dass die Anzahl aller vorhandenen ambigen Ideale l^t beträgt.

Ist $\mathfrak{C}$ ein Ideal aus einer Klasse C des Kummer'schen Körpers K, so werde die durch das relativ conjugirte Ideal $S\mathfrak{C}$ bestimmte Ideal-

klasse mit SC bezeichnet. Die Klassen $SC, S^2C, \ldots, S^{l-1}C$ sollen die zu C **relativ conjugirten Klassen** heissen. Ist ferner $F(S)$ eine beliebige ganzzahlige Function vom $(l-1)$ten Grade in S, nämlich

$$F(S) = a + a_1 S + a_2 S^2 + \cdots + a_{l-1} S^{l-1},$$

wo $a, a_1, \ldots, a_{l-1}$ ganze rationale Zahlen sind, so werde die durch den Ausdruck

$$C^a (SC)^{a_1} (S^2C)^{a_2} \ldots (S^{l-1}C)^{a_{l-1}}$$

bestimmte Klasse die **$F(S)$te symbolische Potenz** der Klasse C genannt und mit

$$C^{a+a_1 S+a_2 S^2+\cdots+a_{l-1} S^{l-1}} = C^{F(S)}$$

bezeichnet. Endlich heisse eine Idealklasse A des Kummer'schen Körpers K eine **ambige Klasse**, wenn $A = SA$, d. h., wenn ihre $(1-S)$te symbolische Potenz $A^{1-S} = 1$ wird. Die $l$te Potenz einer beliebigen ambigen Klasse A ist stets eine solche Klasse, welche unter ihren Idealen in $k(\zeta)$ liegende Ideale enthält. Dies ergiebt sich unmittelbar, wenn wir berücksichtigen, dass wir

$$A^l = A^{1+S+S^2+\cdots+S^{l-1}}$$

als Folge von $A = SA$ haben und dass andererseits die Relativnorm eines beliebigen Ideals in K stets notwendig ein Ideal in $k(\zeta)$ ist.

§ 145.

Der Begriff der Klassenschar im regulären Kummer'schen Körper.

Es sei in dem regulären Kummer'schen Körper K ein solches System von Klassen vorgelegt, dass in der $l$ten Potenz einer jeden dieser Klassen stets Ideale des Körpers $k(\zeta)$ vorkommen, und überdies sollen insbesondere alle diejenigen Klassen, in welchen Ideale des Körpers $k(\zeta)$ vorkommen, dem Systeme angehören; endlich sollen das Product und der Quotient von irgend zwei Klassen des Systems stets wiederum dem Systeme angehören. Ein solches System von Klassen nenne ich eine **Klassenschar des Kummer'schen Körpers.** In einer vorgelegten Klassenschar kann man stets eine gewisse Anzahl n von Klassen $C_1, \ldots, C_n$ bestimmen von der Beschaffenheit, dass man jede Klasse der Klassen-

schar und jede nur einmal erhält, wenn man in dem Ausdruck

$$C_1^{u_1} C_2^{u_2} \dots C_n^{u_n} c$$

einem jeden der Exponenten $u_1, u_2, \dots, u_n$ unabhängig von den anderen alle Werte 0, 1, ..., $l-1$ erteilt, und für c eine jede solche Klasse setzt, welche unter ihren Idealen in $k(\zeta)$ liegende Ideale enthält. Die Klassen $C_1, C_2, \dots, C_n$ mögen dann eine **Basis der Klassenschar** heissen. Es lässt sich leicht zeigen, dass für eine jede andere Basis der Klassenschar die Anzahl n der Klassen, aus welchen die Schar besteht, die gleiche sein muss. Diese Zahl n heisse der **Grad der Klassenschar.**

Enthalten insbesondere alle Klassen einer Schar Ideale des Körpers $k(\zeta)$, so ist die Schar vom Grade 0. Des Weiteren ist beispielsweise die Gesamtheit aller derjenigen Klassen in K, in welchen, sei es ambige Ideale in K, sei es Producte aus ambigen Idealen in K mit Idealen des Körpers $k(\zeta)$ vorkommen, eine Klassenschar. Ferner bildet die Gesamtheit aller ambigen Klassen des Kummer'schen Körpers eine Klassenschar.

§ 146.

Zwei allgemeine Hülfssätze über die relativen Grundeinheiten eines relativ-cyklischen Körpers von ungeradem Primzahlgrade.

Bevor wir die Untersuchungen des vorigen Paragraphen fortsetzen, leiten wir zwei Hülfssätze ab, die sich an den Satz 91 in § 55 anschliessen und wie folgt lauten:

Hülfssatz 31. Es sei der Relativgrad l eines relativ cyklischen Körpers K in Bezug auf einen Unterkörper k eine ungerade Primzahl, ferner sei S eine von der identischen verschiedene Substitution der Relativgruppe von K in Bezug auf k und $H_1, \dots, H_{r+1}$ ein System von relativen Grundeinheiten des Körpers K in Bezug auf k, dann gilt für eine beliebige Einheit E in K jedesmal eine Gleichung von der Gestalt

$$E^f = H_1^{F_1(S)} \dots H_{r+1}^{F_{r+1}(S)} [\varepsilon],$$

wo f ein ganzer rationaler, nicht durch l teilbarer Exponent ist, $F_1(S), \dots$ ..., $F_{r+1}(S)$ ganzzahlige Functionen vom $(l-2)$ten Grade in S bezeichnen und $[\varepsilon]$ eine Einheit in K bedeutet, deren $l$te Potenz in k liegt.

Beweis. Aus dem Beweise des Satzes 91 geht hervor, dass die

Einheiten

$$H_1, \ldots, H_{r+1}, SH_1, \ldots, SH_{r+1}, \ldots, S^{l-2}H_1, \ldots, S^{l-2}H_{r+1}$$

unter Hinzufügung von r Grundeinheiten des Körpers k von einander unabhängig sind, und da die Anzahl dieser Einheiten insgesamt $l(r+1)-1$ beträgt, so giebt es, wenn E eine beliebig angenommene Einheit in K bedeutet, für E gewiss Relationen von der Gestalt

$$(122.)\qquad E^{G(S)} = H_1^{G_1(S)} \ldots H_{r+1}^{G_{r+1}(S)}[\varepsilon],$$

wo $G(S)$, $G_1(S)$, $\ldots$, $G_{r+1}(S)$ ganzzahlige Functionen vom $(l-2)$ten Grade in S sind, unter denen die erste nicht identisch verschwindet, und wo $[\varepsilon]$ eine solche Einheit in K bedeutet, dass $[\varepsilon]^l$ in k liegt. Aus den unendlich vielen vorhandenen Relationen dieser Art denken wir uns eine solche ausgewählt, bei welcher die ganze Function $G(\zeta)$ durch eine möglichst niedrige Potenz von $1-\zeta$ teilbar ist. Wir nehmen an, es treffe dies eben für die Relation (122.) zu; wir setzen zunächst voraus, es sei dabei $G(\zeta)$ noch mindestens einmal durch $1-\zeta$ teilbar. Nach der Definition der Grundeinheiten in § 55 müssen dann

$$G_1(\zeta), \quad \ldots, \quad G_{r+1}(\zeta)$$

sämtlich ebenfalls durch $1-\zeta$ teilbar sein. Erheben wir die Gleichung (122.) in die $(1-S^2)(1-S^3)\ldots(1-S^{l-1})$te symbolische Potenz und setzen

$$G(\zeta) = (1-\zeta)\,G^*(\zeta), \quad G_1(\zeta) = (1-\zeta)\,G_1^*(\zeta), \quad \ldots$$
$$\ldots, \quad G_{r+1}(\zeta) = (1-\zeta)\,G_{r+1}^*(\zeta),$$

so folgt leicht, indem wir berücksichtigen, dass die $(1+S+S^2+\cdots$ $\cdots+S^{l-1})$te symbolische Potenz einer Einheit in K stets eine Einheit in k wird,

$$(123.)\qquad E^{lG^*(S)} = H^{lG_1^*(S)} \ldots H_{r+1}^{lG_{r+1}^*(S)}[\varepsilon],$$

wo $[\varepsilon]$ wieder eine Einheit in k oder die $l$te Wurzel aus einer Einheit in k bedeutet. Wegen der Gleichung (123.) ist eine $l$te Wurzel aus dieser Zahl $[\varepsilon]$ sicherlich eine Zahl in K, also, wie leicht ersichtlich, ebenfalls eine solche Einheit in K, deren $l$te Potenz in k liegt, und die wiederum mit $[\varepsilon]$ zu bezeichnen ist; aus (123.) schliessen wir daher:

$$E^{G^*(S)} = H_1^{G_1^*(S)} \ldots H_{r+1}^{G_{r+1}^*(S)}[\varepsilon],$$

wo wiederum $[\varepsilon]$ eine Einheit in K bedeutet, deren $l$te Potenz in k liegt. Diese Gleichung ist von der nämlichen Gestalt wie (122.), nur dass hier $G^*(\zeta)$ durch eine niedrigere Potenz von $1-\zeta$ teilbar wäre als oben $G(\zeta)$. Dadurch erhalten wir einen Widerspruch mit unserer Annahme, wonach die zu Grunde gelegte Relation (122.) bereits eine solche war, in der $G(\zeta)$ eine möglichst niedrige Potenz von $1-\zeta$ enthielt; wir sehen also, dass unter dieser Voraussetzung in (122.) $G(\zeta)$ nicht durch $1-\zeta$ teilbar sein kann.

Setzen wir

$$f = G(\zeta)G(\zeta^2)\ldots G(\zeta^{l-1}),$$

so wird f eine ganze rationale, nicht durch l teilbare Zahl, und es giebt offenbar zwei ganzzahlige Functionen $H(S)$, $M(S)$, so dass die Gleichung

$$f = H(S)G(S)+M(S)(1+S+S^2+\cdots+S^{l-1})$$

identisch in S erfüllt ist. Erheben wir (122.) in die $H(S)$te symbolische Potenz, so folgt daraus sofort eine Formel von der im Hülfssatz 31 verlangten Beschaffenheit.

Hülfssatz 32. Es mögen dieselben Bezeichnungen wie in Hülfssatz 31 gelten, und überdies bilden wir die Relativnormen der $r+1$ relativen Grundeinheiten des relativ-cyklischen Körpers K, nämlich

$$\eta_1 = N_k(\boldsymbol{H}_1), \quad \ldots, \quad \eta_{r+1} = N_k(\boldsymbol{H}_{r+1}):$$

dann lässt sich jede Einheit ε in k, welche die Relativnorm einer Einheit $\boldsymbol{E}$ des Körpers K ist, in der Gestalt

$$\varepsilon = \eta_1^{u_1}\ldots\eta_{r+1}^{u_{r+1}}[\varepsilon]^l$$

darstellen, wo $u_1, \ldots, u_{r+1}$ ganze rationale Exponenten sind und $[\varepsilon]$ eine Einheit in K ist.

Beweis. Nach Hülfssatz 31 haben wir für $\boldsymbol{E}$ eine Gleichung

$$\boldsymbol{E}^f = \boldsymbol{H}_1^{F_1(S)}\ldots\boldsymbol{H}_{r+1}^{F_{r+1}(S)}[\varepsilon],$$

wo die Zeichen die dort angegebene Bedeutung besitzen. Indem wir von beiden Seiten dieser Gleichung die Relativnorm in Bezug auf k bilden, ergiebt sich

$$\text{(124.)} \qquad \varepsilon^f = \eta_1^{F_1(1)}\ldots\eta_{r+1}^{F_{r+1}(1)}[\varepsilon]^l.$$

Bestimmen wir nun zwei ganze rationale Zahlen a, b, so dass

$$1 = af + bl$$

wird, und erheben dann die Gleichung (124.) in die $a$te Potenz, so entsteht eine Formel von der im Hülfssatz 32 behaupteten Art.

§ 147.

Die durch ambige Ideale bestimmten Idealklassen.

Es sei $K = k(\sqrt[l]{\mu}, \zeta)$ ein regulärer Kummer'scher Körper; wir nehmen aus seiner Relativgruppe die Substitution $S = (\sqrt[l]{\mu} : \zeta\sqrt[l]{\mu})$. Da ein beliebiges ambiges Ideal $\mathfrak{A}$ des Körpers K vermöge seiner Eigenschaft $\mathfrak{A} = S\mathfrak{A}$ stets eine ambige Klasse bestimmt, so haben wir, um zur Kenntniss der ambigen Klassen zu gelangen, vor Allem die aus den ambigen Idealen entspringende Klassenschar zu untersuchen. Wir beweisen die wichtige Thatsache:

Satz 158. *Es sei t die Anzahl der verschiedenen Primideale, welche in der Relativdiscriminante des regulären Kummer'schen Zahlkörpers $K = k(\sqrt[l]{\mu}, \zeta)$ vom Relativgrade l aufgehen; ferner mögen die Relativnormen aller Einheiten von K für $k(\zeta)$ eine Einheitenschar vom Grade m bilden: betrachten wir dann alle diejenigen Klassen, in welchen sei es ambige Ideale des Körpers K, sei es Producte von ambigen Idealen in K mit Idealen in $k(\zeta)$ vorkommen, so bilden diese eine Klassenschar vom Grade*

$$t + m - \frac{l+1}{2}.$$

Beweis. Wir setzen im Folgenden zunächst voraus, dass die Zahl μ nicht von der Gestalt $\varepsilon\alpha^l$ sei, wo ε eine Einheit und α eine Zahl in $k(\zeta)$ bedeuten soll. Es ist dann jede Einheit $[\varepsilon]$ des Körpers $K = k(\sqrt[l]{\mu}, \zeta)$, deren $l$te Potenz in $k(\zeta)$ liegt, notwendig selbst in $k(\zeta)$ gelegen. Nunmehr mögen $H_1, \ldots, H_{\frac{l-1}{2}}$ ein System von relativen Grundeinheiten des Körpers K in Bezug auf $k(\zeta)$ und

$$\eta_1 = N_k(H_1), \quad \ldots, \quad \eta_{\frac{l-1}{2}} = N_k(H_{\frac{l-1}{2}})$$

deren Relativnormen bedeuten.

Wir nehmen erstens an, dass der äusserste Fall $m = \dfrac{l-1}{2}$ ein-

tritt. Aus Hülfssatz 32 schliessen wir dann, dass die Einheiten $\eta_1, \ldots, \eta_{\frac{l-1}{2}}$ eine Basis derjenigen Einheitenschar bilden, welche aus den Relativnormen aller Einheiten in K besteht. Andererseits fassen wir die t ambigen Primideale $\mathfrak{L}_1, \ldots, \mathfrak{L}_t$ des Körpers K ins Auge; dieselben bestimmen t ambige Idealklassen, die wir bez. $L_1, \ldots, L_t$ nennen wollen. Um für die aus diesen Klassen entspringende Klassenschar den Grad zu bestimmen, setzen wir

$$(125.) \qquad \boldsymbol{M} = \sqrt[l]{\mu} = \mathfrak{L}_1^{a_1} \ldots \mathfrak{L}_t^{a_t} \mathfrak{j},$$

wo $a_1, \ldots, a_t$ gewisse ganze rationale Exponenten bedeuten, und wo $\mathfrak{j}$ ein Ideal in $k(\zeta)$ ist. Wegen der zu Anfang getroffenen Voraussetzung über μ ist wenigstens einer der Exponenten $a_1, \ldots, a_t$ nicht durch l teilbar; es sei etwa a_t prim zu l. Wir entnehmen aus der Gleichung (125.), dass

$$c = L_1^{a_1} \ldots L_t^{a_t}$$

eine solche Klasse ist, die Ideale des Körpers $k(\zeta)$ enthält; da L_t^l ebenfalls eine Klasse dieser Art ist, so folgt hieraus sofort, dass die Klasse L_t sich als Product von Potenzen der Klassen $L_1, \ldots, L_{t-1}$ und einer Klasse darstellen lässt, die Ideale des Körpers $k(\zeta)$ enthält.

Wir beweisen jetzt, dass aus den Idealklassen $L_1, \ldots, L_{t-1}$ allein keine Klasse von der Gestalt

$$(126.) \qquad c' = L_1^{a'_1} \ldots L_{t-1}^{a'_{t-1}}$$

hervorgehen kann, welche Ideale des Körpers $k(\zeta)$ enthält, während $a'_1, \ldots, a'_{t-1}$ ganze rationale, nicht sämtlich durch l teilbare Exponenten sind. In der That, auf Grund der Relation (126.) würden wir eine Gleichung

$$(127.) \qquad \boldsymbol{M}' = \mathfrak{L}_1^{a'_1} \ldots \mathfrak{L}_{t-1}^{a'_{t-1}} \mathfrak{j}'$$

aufstellen können, so dass $\mathfrak{j}'$ ein Ideal des Körpers $k(\zeta)$ und $\boldsymbol{M}'$ eine ganze Zahl des Körpers K ist; hieraus schliessen wir dann, dass $\boldsymbol{E} = \boldsymbol{M}'^{1-S}$ eine Einheit in K sein müsste. Auf diese Einheit $\boldsymbol{E}$ wenden wir den Hülfssatz 31 an und erhalten so eine Gleichung von der Gestalt

$$(128.) \qquad \boldsymbol{E}^f = \boldsymbol{H}_1^{F_1(S)} \ldots \boldsymbol{H}_{\frac{l-1}{2}}^{F_{\frac{l-1}{2}}(S)} \varepsilon,$$

wo f eine ganze rationale, nicht durch l teilbare Zahl, $F_1(S), \ldots, F_{\frac{l-1}{2}}(S)$ ganzzahlige Functionen von S und ε eine Einheit in $k(\zeta)$ bedeuten. Da offenbar $N_k(\boldsymbol{E}) = 1$ ist, so ergiebt sich durch Bildung der Relativnorm auf beiden Seiten von (128.) die Gleichung

$$1 = \eta_1^{F_1(1)} \ldots \eta_{\frac{l-1}{2}}^{F_{\frac{l-1}{2}}(1)} \varepsilon^l.$$

Da $\eta_1, \ldots, \eta_{\frac{l-1}{2}}$ eine Basis einer Einheitenschar bilden sollen, so müssen die ganzen rationalen Zahlen $F_1(1), \ldots, F_{\frac{l-1}{2}}(1)$ sämtlich durch l und demnach die ganzen Zahlen $F_1(\zeta), \ldots, F_{\frac{l-1}{2}}(\zeta)$ sämtlich durch $1-\zeta$ teilbar sein. Setzen wir

$$F_1(\zeta) = (1-\zeta) F_1^*(\zeta), \quad \ldots, \quad F_{\frac{l-1}{2}}(\zeta) = (1-\zeta) F_{\frac{l-1}{2}}^*(\zeta)$$

und

$$\boldsymbol{H} = \boldsymbol{H}_1^{F_1^*(S)} \ldots \boldsymbol{H}_{\frac{l-1}{2}}^{F^*_{\frac{l-1}{2}}(S)},$$

so wird

$$\boldsymbol{E}^f = \boldsymbol{H}^{1-S} \varepsilon^*,$$

wo ε^* wieder eine Einheit in $k(\zeta)$ bedeutet. Durch Bildung der Relativnorm folgt aus letzterer Gleichung $1 = \varepsilon^{*l}$, d. h. ε^* ist eine $l$te Einheitswurzel, etwa $= \zeta^g$. Berücksichtigen wir $\boldsymbol{M}^{1-S} = \zeta^{-1}$, so haben wir

$$\{\boldsymbol{M}'^f \boldsymbol{M}^g \boldsymbol{H}^{-1}\}^{1-S} = 1,$$

d. h. der Ausdruck $\boldsymbol{M}'^f \boldsymbol{M}^g \boldsymbol{H}^{-1}$ stellt eine Zahl in $k(\zeta)$ dar. Da nun $\boldsymbol{M}'$ wegen (127.) das Ideal $\mathfrak{L}_t$ nicht oder zu einem durch l teilbaren Exponenten erhoben enthält, $\boldsymbol{M}$ dagegen das Ideal $\mathfrak{L}_t$ in einer Potenz enthält, deren Exponent a_t nicht durch l teilbar ist, so zeigt die Zerlegung dieser Zahl in Primideale des Körpers $k(\zeta)$ erstens, dass g durch l teilbar sein muss; dann zeigt sie weiter, da f zu l prim ist, dass die Exponenten $a_1', \ldots, a_{t-1}'$ sämtlich durch l teilbar sein müssten, was der Voraussetzung widerspricht. Daraus folgt, dass zwischen den Klassen $L_1, \ldots, L_{t-1}$ eine Relation wie (126.) nicht bestehen kann, d. h. die Klassen $L_1, \ldots, L_{t-1}$ bilden unter der gegenwärtigen Annahme, die wesentlich auf $m = \frac{l-1}{2}$ hinauskommt, für die aus allen

ambigen Idealen entspringende Klassenschar eine Basis; der Grad dieser Klassenschar ist daher gleich $t-1$, wie es unserem Satze 158 für $m=\frac{l-1}{2}$ entspricht.

Wir nehmen zweitens $m=\frac{l-3}{2}$ an; dann muss zwischen den Einheiten $\eta_1, \ldots, \eta_{\frac{l-1}{2}}$ eine Relation von der Gestalt $\eta_1^{e_1} \ldots \eta_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}} = \eta^l$ bestehen, wo die Exponenten $e_1, \ldots, e_{\frac{l-1}{2}}$ ganze rationale, nicht sämtlich durch l teilbare Zahlen sind und η eine Einheit in $k(\zeta)$ bedeutet. Ist etwa $e_{\frac{l-1}{2}}$ nicht durch l teilbar, so sind, wie man aus Hülfssatz 32 schliesst, notwendig $\eta_1, \ldots, \eta_{\frac{l-3}{2}}$ eine Basis der aus den Relativnormen aller Einheiten in K gebildeten Einheitenschar. Wir bilden nun die Einheit

$$(129.) \qquad E = H_1^{e_1} \ldots H_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}} \eta^{-1}.$$

Da diese die Relativnorm 1 besitzt, so giebt es nach Satz 90 (S. 272) eine ganze Zahl A in K von der Beschaffenheit, dass $E = A^{1-S}$ wird. Wir bestimmen nun, was jedenfalls möglich ist, eine ganze rationale positive Zahl r in der Weise, dass in dem Product $M' = A M^r$ das Primideal $\mathfrak{L}_t$ zu einem durch l teilbaren Exponenten erhoben vorkommt. Es dürfen dann in M' nicht auch die Factoren $\mathfrak{L}_1, \ldots, \mathfrak{L}_{t-1}$ sämtlich in solchen Potenzen, deren Exponenten durch l teilbar sind, vorkommen, da man sonst unter Benutzung von Satz 153 (S. 429) $M' = \Theta \alpha$ hätte in der Art, dass Θ eine Einheit in K und α eine ganze Zahl in $k(\zeta)$ bedeutet; dann aber würde $\Theta^{1-S} = E \zeta^{-r}$ folgen, und dies widerspräche mit Rücksicht auf (129.), da $e_{\frac{l-1}{2}}$ zu l prim ist, der Definition der relativen Grundeinheiten $H_1, \ldots, H_{\frac{l-1}{2}}$ nach § 55. Es komme nun in M' etwa das ambige Primideal $\mathfrak{L}_{t-1}$ zu einem nicht durch l teilbaren Exponenten erhoben vor. Dann entnehmen wir aus diesem Umstande die Thatsache, dass die Klasse L_{t-1} sich als Product von Potenzen der Klassen $L_1, \ldots, L_{t-2}$ und einer solchen Klasse darstellen lässt, die Ideale des Körpers $k(\zeta)$ enthält.

Wir beweisen jetzt, dass aus den Idealklassen $L_1, \ldots, L_{t-2}$ keine Klasse

$$(130.)\qquad c'' = L_1^{a''_1} \ldots L_{t-2}^{a''_{t-2}}$$

hervorgehen kann, welche Ideale in $k(\zeta)$ enthält, während die Exponenten $a''_1, \ldots, a''_{t-2}$ ganze rationale, nicht sämtlich durch l teilbare Zahlen sind. In der That, eine Relation (130.) hätte eine Gleichung von der Gestalt

$$(131.)\qquad \boldsymbol{M}'' = \mathfrak{L}_1^{a''_1} \ldots \mathfrak{L}_{t-2}^{a''_{t-2}} \mathfrak{j}''$$

zur Folge von der Art, dass $\boldsymbol{M}''$ eine ganze Zahl in K und $\mathfrak{j}''$ ein Ideal in $k(\zeta)$ ist; hieraus schliessen wir dann, dass $\boldsymbol{E}' = \boldsymbol{M}''^{1-S}$ eine Einheit in K sein müsste. Wir wenden für diese Einheit $\boldsymbol{E}'$ den Hülfssatz 31 an und erhalten so eine Gleichung

$$(132.)\qquad \boldsymbol{E}'^{f'} = \boldsymbol{H}_1^{F'_1(S)} \ldots \boldsymbol{H}_{\frac{l-1}{2}}^{F'_{\frac{l-1}{2}}(S)} \varepsilon,$$

wo f' eine ganze rationale, nicht durch l teilbare Zahl,

$$F'_1(S), \quad \ldots, \quad F'_{\frac{l-1}{2}}(S)$$

ganzzahlige Functionen von S sind und ε eine Einheit in $k(\zeta)$ ist. Wir bestimmen nun einen ganzen rationalen Exponenten u in der Weise, dass die ganze Zahl $F'_{\frac{l-1}{2}}(1) + u e_{\frac{l-1}{2}}$ durch l teilbar wird; mit Rücksicht auf $N_k(\boldsymbol{E}') = 1$ erhalten wir aus (132.) durch Bildung der Relativnorm in Bezug auf $k(\zeta)$ die Gleichung:

$$(133.)\qquad 1 = \eta_1^{F'_1(1) + u e_1} \ldots \eta_{\frac{l-3}{2}}^{F'_{\frac{l-3}{2}}(1) + u e_{\frac{l-3}{2}}} \varepsilon'^{l},$$

wo ε' wiederum eine Einheit in $k(\zeta)$ ist. Da die Einheiten $\eta_1, \ldots, \eta_{\frac{l-3}{2}}$ eine Basis einer Einheitenschar sind, so folgt aus (133.), dass die Exponenten $F'_1(1) + u e_1, \ldots, F'_{\frac{l-3}{2}}(1) + u e_{\frac{l-3}{2}}$ sämtlich durch l, d. h. die Zahlen $F'_1(\zeta) + u e_1, \ldots, F'_{\frac{l-3}{2}}(\zeta) + u e_{\frac{l-3}{2}}$ sämtlich durch $1-\zeta$

teilbar sein müssen. Setzen wir

$$F'_1(\zeta)+ue_1 = (1-\zeta)F'^{*}_1(\zeta), \quad \ldots$$
$$\ldots, \quad F'_{\frac{l-1}{2}}(\zeta)+ue_{\frac{l-1}{2}} = (1-\zeta)F'^{*}_{\frac{l-1}{2}}(\zeta)$$

und

$$H' = H_1^{F'^{*}_1(S)} \ldots H_{\frac{l-1}{2}}^{F'^{*}_{\frac{l-1}{2}}(S)},$$

so folgt aus (132.)

$$E'^{f'}E^u = H'^{1-S}\varepsilon'^{*},$$

wo E die durch (129.) festgelegte Einheit in K und ε'^{*} wieder eine Einheit in $k(\zeta)$ bedeutet; durch Bildung der Relativnorm erhalten wir $1=\varepsilon'^{*l}$, d. h. ε'^{*} ist eine $l$te Einheitswurzel, etwa gleich $\zeta^{g'}$. Alsdann wird, wenn wir die Gleichungen

$$M^{1-S}=\zeta^{-1}, \quad M'^{1-S}=E\zeta^{-r}, \quad M''^{1-S}=E'$$

berücksichtigen,

$$\{M''^{f'}M'^{u}M^{g'-ur}H'^{-1}\}^{1-S} = 1,$$

d. h. der Ausdruck $M''^{f'}M'^{u}M^{g'-ur}H'^{-1}$ stellt eine Zahl in $k(\zeta)$ dar. Beachten wir, dass $\mathfrak{L}^l_t, \mathfrak{L}^l_{t-1}, \mathfrak{L}^l_{t-2}, \ldots, \mathfrak{L}^l_1$ in $k(\zeta)$ Primideale sind, so schliessen wir daraus zunächst, dass $g'-ur$ durch l teilbar sein muss; sodann ersehen wir, da M' nach Voraussetzung das Ideal $\mathfrak{L}_{t-1}$ zu einer Potenz erhoben enthält, deren Exponent nicht durch l teilbar ist, dagegen in der Zahl M'' wegen (131.) das Ideal $\mathfrak{L}_{t-1}$ sicher zu einem durch l teilbaren Exponenten erhoben vorkommt, dass notwendigerweise auch u durch l teilbar sein muss, und endlich müssten dann, da f' zu l prim ist, die Exponenten $a''_1, \ldots, a''_{t-2}$ sämtlich durch l teilbar sein, was unserer Voraussetzung über dieselben widerspricht. Damit ist gezeigt, dass zwischen den Klassen $L_1, \ldots, L_{t-2}$ eine Relation wie (130.) nicht bestehen kann, d. h. die Klassen $L_1, \ldots, L_{t-2}$ bilden unter der gegenwärtigen Annahme $\mathring{m}=\frac{l-3}{2}$ für die aus allen ambigen Idealen entspringende Klassenschar eine Basis; der Grad dieser Klassenschar ist daher gleich $t-2$, wie es unserem Satz 158 entspricht.

Wenn wir drittens $m=\frac{l-5}{2}$ annehmen, so besteht zwischen

den Einheiten $\eta_1, \ldots, \eta_{\frac{l-1}{2}}$ nicht nur, wie im vorigen Falle, eine Relation von der Gestalt $\eta_1^{e_1} \ldots \eta_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}} = \eta^l$, wo η eine Einheit in $k(\zeta)$ und einer der Exponenten $e_1, \ldots, e_{\frac{l-1}{2}}$, etwa wieder $e_{\frac{l-1}{2}}$, nicht durch l teilbar ist, sondern es besteht alsdann noch eine zweite Relation von der Gestalt $\eta_1^{e'_1} \ldots \eta_{\frac{l-3}{2}}^{e'_{\frac{l-3}{2}}} = \eta'^l$, wo η' wieder eine Einheit in $k(\zeta)$ ist, und wo einer der Exponenten $e'_1, \ldots, e'_{\frac{l-3}{2}}$, etwa $e'_{\frac{l-3}{2}}$, nicht durch l teilbar ist. Wir bilden die Einheiten

$$(134.)\qquad \left\{\begin{aligned} \boldsymbol{E} &= \boldsymbol{H}_1^{e_1} \ldots \boldsymbol{H}_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}} \eta^{-1}, \\ \boldsymbol{E}' &= \boldsymbol{H}_1^{e'_1} \ldots \boldsymbol{H}_{\frac{l-3}{2}}^{e'_{\frac{l-3}{2}}} \eta'^{-1}. \end{aligned}\right.$$

Da die Relativnormen der Einheiten $\boldsymbol{E}$ und $\boldsymbol{E}'$ gleich 1 sind, so können wir nach Satz 90 (S. 272) $\boldsymbol{E} = \boldsymbol{A}^{1-S}$ und $\boldsymbol{E}' = \boldsymbol{A}'^{1-S}$ setzen, wobei $\boldsymbol{A}$ und $\boldsymbol{A}'$ ganze Zahlen in K bedeuten. Bestimmen wir dann zunächst, wie im vorigen Falle, eine ganze rationale positive Zahl r derart, dass $\boldsymbol{M}' = \boldsymbol{A}\boldsymbol{M}^r$ den Factor $\mathfrak{L}_t$ zu einem durch l teilbaren Exponenten erhoben enthält, so kommt, wie die dortigen Ueberlegungen zeigen, in $\boldsymbol{M}'$ mindestens eines der ambigen Primideale $\mathfrak{L}_1, \ldots, \mathfrak{L}_{t-1}$ zu einer Potenz erhoben vor, deren Exponent nicht durch l teilbar ist; es treffe dies etwa für $\mathfrak{L}_{t-1}$ zu. Wir bestimmen dann zwei ganze rationale positive Zahlen r' und r'' so, dass die Zahl $\boldsymbol{M}'' = \boldsymbol{A}'\boldsymbol{M}'^{r'}\boldsymbol{M}^{r''}$ die beiden Factoren $\mathfrak{L}_t$ und $\mathfrak{L}_{t-1}$ zu Exponenten erhoben enthält, die durch l teilbar sind. Alsdann können in dieser Zahl $\boldsymbol{M}''$ die Factoren $\mathfrak{L}_1, \ldots, \mathfrak{L}_{t-2}$ nicht sämtlich zu solchen Potenzen erhoben vorkommen, deren Exponenten durch l teilbar sind. Denn wäre dies der Fall, so könnten wir unter Benutzung von Satz 153 $\boldsymbol{M}'' = \boldsymbol{\Theta}'\alpha'$ setzen, so dass $\boldsymbol{\Theta}'$ eine Einheit in K und α' eine ganze Zahl in $k(\zeta)$ ist. Berücksichtigen wir dann die Gleichungen $\boldsymbol{M}^{1-S} = \zeta^{-1}$, $\boldsymbol{A}^{1-S} = \boldsymbol{E}$, $\boldsymbol{A}'^{1-S} = \boldsymbol{E}'$, so wäre

$$\boldsymbol{\Theta}'^{1-S} = \boldsymbol{E}'\boldsymbol{E}^{r'}\zeta^{-(rr'+r'')};$$

wegen (134.) würde hieraus folgen:

$$(135.)\qquad \Theta'^{1-S} = H_1^{e'_1+r'e_1} \ldots H_{\frac{l-3}{2}}^{e'_{\frac{l-3}{2}}+r'e_{\frac{l-3}{2}}} H_{\frac{l-1}{2}}^{r'e_{\frac{l-1}{2}}}\, \varepsilon,$$

wo ε eine gewisse Einheit in $k(\zeta)$ bedeutet; diese Relation widerspräche aber der Definition der relativen Grundeinheiten nach § 55; denn da jede der beiden Zahlen $e_{\frac{l-1}{2}}$, $e'_{\frac{l-3}{2}}$ zu l prim ist, so sind die Exponenten von $H_{\frac{l-3}{2}}$, $H_{\frac{l-1}{2}}$ in (135.) sicher niemals beide zugleich durch l teilbar. Kommt nun in M'' etwa $\mathfrak{L}_{t-2}$ zu einem nicht durch l teilbaren Exponenten erhoben vor, so entnehmen wir aus diesem Umstande, dass die Klasse L_{t-2} sich als Product von Potenzen der Klassen $L_1, \ldots, L_{t-3}$ und einer solchen Klasse darstellen lässt, die Ideale des Körpers $k(\zeta)$ enthält.

Durch die entsprechenden Ueberlegungen wie im vorigen Falle $m = \frac{l-3}{2}$ kann man nun unter der gegenwärtigen Annahme $m = \frac{l-5}{2}$ beweisen, dass aus den Idealklassen $L_1, \ldots, L_{t-3}$ keine Klasse

$$c''' = L_1^{a'''_1} \ldots L_{t-3}^{a'''_{t-3}}$$

hervorgehen kann, welche Ideale in $k(\zeta)$ enthält, während die Exponenten $a'''_1, \ldots, a'''_{t-3}$ ganze rationale, nicht sämtlich durch l teilbare Zahlen sind. Wir ersehen dann, dass bei der gegenwärtigen Annahme $L_1, \ldots, L_{t-3}$ eine Basis der aus den ambigen Idealen entspringenden Klassenschar bilden; der Grad dieser Klassenschar beträgt folglich $t-3$, wie es dem Satz 158 entspricht.

Durch die geeignete Weiterführung des oben geschilderten Verfahrens gelangen wir zum vollständigen Beweise des Satzes 158.

Wir hatten oben den Fall ausgeschlossen, dass der Kummer'sche Körper K durch eine Zahl $\sqrt[l]{\varepsilon}$ bestimmt werden kann, wo ε eine Einheit in $k(\zeta)$ bedeutet; wir haben daher diesen Fall jetzt noch besonders zu behandeln. Die Relativdiscriminante des Körpers $K = k(\sqrt[l]{\varepsilon}, \zeta)$ kann alsdann nach Satz 148 keine anderen Primfactoren als $\mathfrak{l}$ enthalten; nach Satz 94 und Satz 153 muss sie den Factor $\mathfrak{l}$ wirklich enthalten. Wir haben dann in K eine Zerlegung $\mathfrak{l} = \mathfrak{L}^l$, und es ist $\mathfrak{L}$ das einzige ambige Primideal des Körpers K. Es seien wieder $\eta_1, \ldots, \eta_{\frac{l-1}{2}}$ bez.

die Relativnormen der $\frac{l-1}{2}$ relativen Grundeinheiten $H_1, \ldots, H_{\frac{l-1}{2}}$. Da der Grad einer Einheitenschar in $k(\zeta)$ stets $\leqq \frac{l-1}{2}$ ist, so besteht sicher eine Relation von der Gestalt:

(136.) $$\eta_1^{e_1} \cdots \eta_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}} \varepsilon^{e_{\frac{l+1}{2}}} = \eta^l,$$

wo $e_1, \ldots, e_{\frac{l-1}{2}}, e_{\frac{l+1}{2}}$ ganze rationale, nicht sämtlich durch l teilbare Exponenten sind, und wo η eine Einheit in $k(\zeta)$ bedeutet. Setzen wir

(137.) $$H = H_1^{e_1} \cdots H_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}} \left(\sqrt[l]{\varepsilon}\right)^{e_{\frac{l+1}{2}}} \eta^{-1},$$

so ist $N_k(H) = 1$ und folglich nach Satz 90 $H = A^{1-S}$, wo A eine geeignete ganze Zahl in K bedeutet; wir können dann $A = \mathfrak{L}^a \mathfrak{j}$ setzen, wo $\mathfrak{L}^a$ eine Potenz des ambigen Primideals $\mathfrak{L}$ und $\mathfrak{j}$ ein Ideal in $k(\zeta)$ bedeutet. Der Exponent a ist dann sicher nicht durch l teilbar; denn sonst wäre wegen $\mathfrak{L}^l = \mathfrak{l} = 1-\lambda$ und mit Rücksicht auf Satz 153 $A = \Theta\alpha$ in solcher Weise, dass Θ eine Einheit in K und α eine Zahl in $k(\zeta)$ bezeichnet; hieraus aber würden wir $H = \Theta^{1-S}$ entnehmen und dadurch mit Rücksicht auf (137.) in einen Widerspruch mit der Definition der relativen Grundeinheiten in § 55 geraten. Aus der Gleichung $A = \mathfrak{L}^a \mathfrak{j}$ schliessen wir $\mathfrak{j}^l \sim 1$, daraus $\mathfrak{j} \sim 1$, $\mathfrak{L}^a \sim 1$ und, da a zu l prim ist, $\mathfrak{L} \sim 1$, d. h. das einzige im gegenwärtigen Fall vorhandene ambige Ideal $\mathfrak{L}$ ist ein Hauptideal; der Grad der aus den ambigen Idealen entspringenden Klassenschar ist mithin gleich 0.

Wir nehmen nun an, von den Exponenten $e_1, \ldots, e_{\frac{l-1}{2}}$ sei etwa $e_{\frac{l-1}{2}}$ prim zu l, und beweisen dann, dass keine Relation

(138.) $$\eta_1^{e'_1} \cdots \eta_{\frac{l-3}{2}}^{e'_{\frac{l-3}{2}}} \varepsilon^{e'_{\frac{l+1}{2}}} = \eta'^l$$

bestehen kann von der Art, dass $e'_1, \ldots, e'_{\frac{l-3}{2}}, e'_{\frac{l+1}{2}}$ ganze rationale, nicht sämtlich durch l teilbare Exponenten sind und η' eine Einheit in $k(\zeta)$ bedeutet. In der That, würde eine solche Relation (138.) gelten,

so hätten wir in

$$H' = H_1^{e'_1} \ldots H_{\frac{l-3}{2}}^{e'_{\frac{l-3}{2}}} (\sqrt[l]{\varepsilon})^{e'_{\frac{l+1}{2}}} \eta'^{-1}$$

eine Einheit mit der Relativnorm 1. Wir setzen unter Benutzung des Satzes 90 $H' = A'^{1-S}$, wo A' eine geeignete ganze Zahl in K bedeutet, und bestimmen dann einen solchen ganzen rationalen positiven Exponenten r, dass in $A'A^r$ das Primideal $\mathfrak{L}$ zu einem durch l teilbaren Exponenten vorkommt. Nunmehr können wir mit Rücksicht auf Satz 153 $A'A^r = \Theta'\alpha'$ setzen in solcher Weise, dass Θ' eine Einheit in K und α' eine ganze Zahl in $k(\zeta)$ bedeutet; dann wird $\Theta'^{1-S} = H'H^r$, d. h. die Einheit

$$H_1^{e'_1+re_1} \ldots H_{\frac{l-3}{2}}^{e'_{\frac{l-3}{2}}+re_{\frac{l-3}{2}}} H_{\frac{l-1}{2}}^{re_{\frac{l-1}{2}}} (\sqrt[l]{\varepsilon})^{e'_{\frac{l+1}{2}}+re_{\frac{l+1}{2}}} \eta'^{-1}\eta^{-r}$$

wäre die symbolische $(1-S)$te Potenz einer Einheit in K, und diese Folgerung steht mit der Definition der relativen Grundeinheiten aus dem schon mehrfach erörterten Grunde in Widerspruch. Damit ist gezeigt, dass eine Relation wie (138.) nicht statthaben kann; mit Rücksicht auf (136.) und auf den Umstand, dass $e_{\frac{l-1}{2}}$ zu l prim ist, bilden nunmehr $\eta_1, \ldots, \eta_{\frac{l-3}{2}}, \varepsilon$ eine Basis der aus den Relativnormen aller Einheiten in K gebildeten Einheitenschar; es folgt also, dass der Grad m dieser Schar gleich $\frac{l-1}{2}$ ist und somit jede Einheit in $k(\zeta)$ die Relativnorm einer Einheit in K ist. Es ist demnach

$$t + m - \frac{l+1}{2} = 0$$

und damit der Satz 158 auch in diesem Falle bestätigt.

§ 148.

Die sämtlichen ambigen Idealklassen.

Der Satz 158 hat eine merkwürdige Beziehung aufgedeckt, die zwischen der aus den ambigen Idealen entspringenden Klassenschar und derjenigen Einheitenschar stattfindet, die aus den Relativnormen sämtlicher Einheiten in K gebildet wird. Eine ebenso wichtige Beziehung herrscht zwischen der aus allen ambigen Klassen gebildeten

Klassenschar und einer gewissen Einheitenschar in $k(\zeta)$. Wir sprechen folgenden Satz aus:

Satz 159. Es sei t die Anzahl der Primideale, die in der Relativdiscriminante des regulären Kummer'schen Körpers K vom Relativgrade l aufgehen; ferner mögen alle diejenigen Einheiten in $k(\zeta)$, welche gleich Relativnormen sei es von Einheiten, sei es von gebrochenen Zahlen des Körpers K sind, eine Einheitenschar vom Grade n bilden: dann besitzt die aus sämtlichen ambigen Klassen bestehende Klassenschar den Grad $t+n-\frac{l+1}{2}$.

Beweis. Es habe m die Bedeutung wie in Satz 158. Fällt erstens $n=m$ aus, so stimmt die jetzt in Frage kommende Einheitenschar mit der in Satz 158 behandelten Einheitenschar überein, d. h. wenn eine Einheit in $k(\zeta)$ gleich der Relativnorm einer gebrochenen Zahl in K ist, so ist sie stets auch gleich der Relativnorm einer Einheit in K. Wir beweisen nun, dass in diesem Falle die Klassenschar, die aus den ambigen Idealen entspringt, die Schar sämtlicher ambigen Klassen darstellt. In der That, wenn A eine beliebige ambige Klasse in K und $\mathfrak{A}$ ein Ideal aus A ist, so können wir $\mathfrak{A}^{1-S}=A$ setzen in solcher Weise, dass A eine geeignete ganze oder gebrochene Zahl in K bedeutet, und die Relativnorm $N_k(A)$ wird dann offenbar gleich einer Einheit ϑ des Körpers $k(\zeta)$. Da dann unter der gegenwärtigen Annahme $n=m$ nach dem soeben Bemerkten auch eine Einheit H in K gefunden werden kann derart, dass $N_k(H)=\vartheta$ wird, so haben wir $N_k(A^{-1}H)=1$ und folglich nach Satz 90 $A^{-1}H=B^{1-S}$ oder $AB^{1-S}=H$, wo B eine geeignete ganze Zahl in K ist. Wegen $A=\mathfrak{A}^{1-S}$ wird $(\mathfrak{A}B)^{1-S}=1$, d. h. es ist $\mathfrak{A}B$ gleich dem Producte aus einem ambigen Ideal und einem Ideal in $k(\zeta)$, und es entsteht also die Klasse A durch Multiplication einer Klasse, die ein ambiges Ideal enthält, mit einer Klasse, die Ideale in $k(\zeta)$ enthält. Damit ist unsere Behauptung bewiesen und der Grad der aus sämtlichen ambigen Klassen gebildeten Klassenschar ist nunmehr mit Rücksicht auf Satz 158 gleich

$$t+m-\frac{l+1}{2},$$

wie es im vorliegenden Falle $n=m$ dem Satz 159 entspricht.

Es sei zweitens $n=m+1$; dann kommt in $k(\zeta)$ eine Einheit ϑ vor, die zwar nicht die Relativnorm einer Einheit in K, aber doch die Relativnorm einer gebrochenen Zahl A in K ist, und es muss sich jede andere Einheit ϑ' von der nämlichen Natur durch die Einheit ϑ solcher

Gestalt $\vartheta' = \vartheta^a \eta$ ausdrücken lassen, dass a ein ganzer rationaler Exponent und η die Relativnorm einer Einheit in K ist. Wir setzen

$$A = \mathfrak{P}_1^{G_1(S)} \ldots \mathfrak{P}_r^{G_r(S)},$$

wo $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ von einander verschiedene Primideale in K bedeuten sollen, von denen keine zwei zu einander relativ conjugirt sind, und wo $G_1(S), \ldots, G_r(S)$ ganzzahlige Functionen vom $(l-1)$ten Grade in S sind. Wegen $N_k(A) = \vartheta$ folgt

$$(\mathfrak{P}_1^{G_1(S)} \ldots \mathfrak{P}_r^{G_r(S)})^{1+S+\cdots+S^{l-1}} = 1,$$

und hieraus entnehmen wir leicht, dass die Functionen $G_1(S), \ldots, G_r(S)$ sämtlich durch $1-S$ teilbar sein müssen. Setzen wir

$$G_1(S) = (1-S)G_1^*(S), \quad \ldots, \quad G_r(S) = (1-S)G_r^*(S)$$

und

$$\mathfrak{P}_1^{G_1^*(S)} \ldots \mathfrak{P}_r^{G_r^*(S)} = \mathfrak{A}\alpha,$$

wo $\mathfrak{A}$ ein Ideal in K und α eine ganze oder gebrochene Zahl in $k(\zeta)$ ist, so wird $A = \mathfrak{A}^{1-S}$. Hieraus folgt zunächst, dass $\mathfrak{A}$ eine ambige Klasse bestimmt. Diese ambige Klasse, sie heisse A, enthält kein Ideal, welches das Product eines ambigen Ideals mit einem Ideal des Körpers $k(\zeta)$ wäre. In der That, wäre dies der Fall, so könnten wir $\mathfrak{A} = \Gamma \mathfrak{L} \mathfrak{j}$ setzen so, dass Γ eine ganze oder gebrochene Zahl in K, ferner $\mathfrak{L}$ ein ambiges Ideal in K und $\mathfrak{j}$ ein Ideal in $k(\zeta)$ bedeutet; dann aber wäre $\mathfrak{A}^{1-S} = \Gamma^{1-S}$, d. h. $A = H\Gamma^{1-S}$, wo H eine Einheit in K ist. Hieraus würde $N_k(A) = N_k(H) = \vartheta$ folgen, was der vorausgesetzten Beschaffenheit der Einheit ϑ widerspricht.

Wir wollen nun für die gegenwärtige Annahme $n = m+1$ den Nachweis führen, dass jede überhaupt vorhandene ambige Klasse A' in der Gestalt $A' = A^a Lc$ dargestellt werden kann, wo A^a eine Potenz der soeben bestimmten Klasse A bedeutet, wo ferner L eine Klasse mit ambigem Ideal und c eine solche Klasse bedeutet, die unter ihren Idealen Ideale des Körpers $k(\zeta)$ enthält. Zu dem Zwecke nehmen wir aus A' ein beliebiges Ideal $\mathfrak{A}'$; dann können wir $\mathfrak{A}'^{1-S} = A'$ setzen in solcher Weise, dass A' eine geeignete ganze oder gebrochene Zahl in K wird. Es ist sodann $N_k(A') = \vartheta'$ eine Einheit in $k(\zeta)$; wir setzen unserer Voraussetzung entsprechend $N_k(A') = \vartheta^a \eta$, wo ϑ, a, η die oben erklärte Bedeutung haben sollen. Es sei A die oben betrachtete Zahl, für welche $\vartheta = N_k(A)$ ist; es sei ferner $\eta = N_k(H)$, wo H eine Einheit in K bedeute. Aus diesen Gleichungen ergiebt

sich $N_k(A'^{-1}A^a H)=1$, und daher wird nach Satz 90 $A'^{-1}A^a H = \Gamma^{1-S}$, wo Γ eine geeignete ganze Zahl in K ist; hieraus entnehmen wir $(\mathfrak{A}'^{-1}\mathfrak{A}^a\Gamma^{-1})^{1-S}=1$. Die letztere Gleichung zeigt, dass $\mathfrak{A}'^{-1}\mathfrak{A}^a\Gamma^{-1}$ nach Multiplication mit einer geeigneten ganzen Zahl des Körpers $k(\zeta)$ das Product eines ambigen Ideals $\mathfrak{L}$ in ein Ideal $\mathfrak{j}$ des Körpers $k(\zeta)$ wird; wir haben somit $\mathfrak{A}' \sim \mathfrak{A}^a\mathfrak{L}\mathfrak{j}$. Es geht daraus in dem vorliegenden Falle $n=m+1$ hervor, dass der Grad der aus sämtlichen ambigen Klassen bestehenden Klassenschar $t+m+1-\frac{l+1}{2}$ beträgt, und dies ist die Aussage des Satzes 159 für diesen Fall.

Nehmen wir drittens $n=m+2$ an, so existirt in $k(\zeta)$ ausser der Einheit ϑ noch eine Einheit ϑ', welche die Relativnorm einer gebrochenen Zahl A' in K ist, und für die dennoch keine Darstellung von der Gestalt $\vartheta'=\vartheta^a\eta$ möglich ist, wo ϑ^a eine Potenz der oben eingeführten Einheit ϑ und η die Relativnorm einer Einheit in K bedeuten soll. Wir setzen

$$A' = \mathfrak{P}_1'^{G_1'(S)} \cdots \mathfrak{P}_{r'}'^{G_{r'}'(S)},$$

wo $\mathfrak{P}_1', \ldots, \mathfrak{P}_{r'}'$ solche Primideale in K bedeuten sollen, von denen keine zwei einander gleich oder relativ conjugirt sind, und wo $G_1'(S), \ldots, G_{r'}'(S)$ ganzzahlige Functionen vom $(l-1)$ten Grade in S sind. Wegen $N_k(A')=\vartheta'$ folgt

$$(\mathfrak{P}_1'^{G_1'(S)} \cdots \mathfrak{P}_{r'}'^{G_{r'}'(S)})^{1+S+\cdots+S^{l-1}} = 1,$$

und hieraus entnehmen wir leicht, dass die Functionen $G_1'(S), \ldots, G_{r'}'(S)$ sämtlich durch $1-S$ teilbar sein müssen. Setzen wir

$$G_1'(S) = (1-S)\,G_1'^*(S), \quad \ldots, \quad G_{r'}'(S) = (1-S)\,G_{r'}'^*(S)$$

und

$$\mathfrak{P}_1'^{G_1'^*(S)} \cdots \mathfrak{P}_{r'}'^{G_{r'}'^*(S)} = \mathfrak{A}'\alpha',$$

so dass $\mathfrak{A}'$ ein Ideal in K und α' eine ganze oder gebrochene Zahl in $k(\zeta)$ ist, so wird $A'=\mathfrak{A}'^{1-S}$. Das Ideal $\mathfrak{A}'$ bestimmt daher eine ambige Klasse A'. Diese Klasse ist nicht in der Gestalt $A'=A^a Lc$ darstellbar, wo A^a eine Potenz der Klasse A, L eine Klasse mit einem ambigen Ideal und c eine Klasse mit Idealen in $k(\zeta)$ bedeutet. In der That, eine solche Darstellung der Klasse A' hätte für das Ideal $\mathfrak{A}'$ eine Darstellung $\mathfrak{A}'=\Gamma\mathfrak{A}^a\mathfrak{L}\mathfrak{j}$ zur Folge, wo Γ eine Zahl in K, ferner $\mathfrak{L}$ ein ambiges Ideal und $\mathfrak{j}$ ein Ideal in $k(\zeta)$ bedeuten soll; dann aber wäre $\mathfrak{A}'^{1-S}=\Gamma^{1-S}\mathfrak{A}^{a(1-S)}=\Gamma^{1-S}A^a$, d. h. $A'=H\Gamma^{1-S}A^a$, wo H eine Einheit in K ist. Durch Bildung der Relativnorm ergäbe sich

nunmehr $N_k(A') = \vartheta' = \vartheta^a N_k(H)$, und das Vorhandensein einer solchen Relation haben wir oben ausgeschlossen.

Bei der gegenwärtigen Annahme $n = m + 2$ muss jede Einheit ϑ'' in $k(\zeta)$, welche die Relativnorm einer Zahl in K ist, in der Gestalt $\vartheta'' = \vartheta'^{a'} \vartheta^a \eta$ darstellbar sein, so dass a', a ganze rationale Exponenten sind und η die Relativnorm einer Einheit in K bedeutet. Indem wir diesen Umstand berücksichtigen, können wir durch ähnliche Ueberlegungen, wie im vorigen Falle $n = m + 1$, zeigen, dass überhaupt jede vorhandene ambige Klasse A'' in der Gestalt $A'^{a'} A^a L c$ sich darstellen lässt, wo A', A die eben bestimmten ambigen Klassen sind und L eine Klasse mit ambigem Ideal, c eine Klasse mit Idealen in $k(\zeta)$ ist. Daraus geht dann hervor, dass der Grad der aus allen ambigen Klassen bestehenden Klassenschaar genau $t + m + 2 - \frac{l+1}{2}$ beträgt, wie es der Satz 159 für den Fall $n = m + 2$ aussagt.

Durch Fortsetzung der eingeleiteten Schlussweise erhalten wir den vollständigen Beweis des Satzes 159.

§ 149.

Das Charakterensystem einer Zahl und eines Ideals im regulären Kummer'schen Körper.

Es handelt sich nun darum, diejenige Einteilung der Idealklassen eines aus dem regulären Kreiskörper $k(\zeta)$ entspringenden Kummer'schen Körpers $K = k(\sqrt[l]{\mu}, \zeta)$ zu erörtern, welche der Einteilung der Klassen eines quadratischen Körpers in Geschlechter entspricht. Wir bezeichnen die verschiedenen in der Relativdiscriminante des Körpers K aufgehenden Primideale des Körpers $k(\zeta)$, deren Anzahl t sei, mit $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$. Zu einer beliebigen ganzen Zahl ν $(\neq 0)$ in $k(\zeta)$ gehören dann bestimmte Werte der t einzelnen Symbole

$$(139.) \qquad \left\{\frac{\nu,\, \mu}{\mathfrak{l}_1}\right\}, \quad \ldots, \quad \left\{\frac{\nu,\, \mu}{\mathfrak{l}_t}\right\};$$

diese Symbole bedeuten $l$te Einheitswurzeln gemäss ihrer Definition in § 131. Diese t Einheitswurzeln (139.) sollen das **Charakterensystem der Zahl** ν im Kummer'schen Körper K heissen. Um auch einem jeden Ideal $\mathfrak{J}$ des Kummer'schen Körpers K in bestimmter

Weise ein Charakterensystem zuzuordnen, bilden wir die Relativnorm $N_k(\mathfrak{J}) = \mathfrak{j}$. Ferner bezeichnen wir mit h der Anzahl die Idealklassen in $k(\zeta)$ und bestimmen eine ganze rationale positive Zahl h^* derart, dass $hh^* \equiv 1$ nach l wird. Dann ist $\mathfrak{j}^{hh^*}$ sicher ein Hauptideal in $k(\zeta)$; wir setzen $\mathfrak{j}^{hh^*} = (\nu)$, wo ν eine ganze Zahl in $k(\zeta)$ sein soll. Nunmehr verstehen wir unter ξ_1 eine Einheit in $k(\zeta)$. Haben dann für jede beliebige Einheit ξ_1 alle t Symbole

$$\left\{\frac{\xi_1, \mu}{\mathfrak{l}_1}\right\}, \quad \ldots, \quad \left\{\frac{\xi_1, \mu}{\mathfrak{l}_t}\right\}$$

durchweg den Wert 1, so setzen wir $r = t$ und bezeichnen die r Einheitswurzeln

$$\left\{\frac{\nu, \mu}{\mathfrak{l}_1}\right\}, \quad \ldots, \quad \left\{\frac{\nu, \mu}{\mathfrak{l}_r}\right\}$$

als das **Charakterensystem des Ideals** $\mathfrak{J}$; dasselbe ist dann durch das Ideal $\mathfrak{J}$ völlig eindeutig bestimmt.

Es sei andererseits eine specielle Einheit ε_1 in $k(\zeta)$ vorhanden, für welche wenigstens eines der t Symbole

$$\left\{\frac{\varepsilon_1, \mu}{\mathfrak{l}_1}\right\}, \quad \ldots, \quad \left\{\frac{\varepsilon_1, \mu}{\mathfrak{l}_t}\right\}$$

von 1 verschieden ausfällt; dann können wir, ohne damit eine Beschränkung einzuführen, annehmen, es sei etwa $\left\{\frac{\varepsilon_1, \mu}{\mathfrak{l}_t}\right\} = \zeta$. Wir betrachten nun alle diejenigen Einheiten ξ_2 in $k(\zeta)$, für welche $\left\{\frac{\xi_2, \mu}{\mathfrak{l}_t}\right\} = 1$ wird. Es sei unter diesen weiter eine solche Einheit $\xi_2 = \varepsilon_2$ vorhanden, für welche wenigstens eines der $t-1$ Symbole

$$\left\{\frac{\varepsilon_2, \mu}{\mathfrak{l}_1}\right\}, \quad \ldots, \quad \left\{\frac{\varepsilon_2, \mu}{\mathfrak{l}_{t-1}}\right\}$$

von 1 verschieden ausfällt; dann können wir annehmen, es sei etwa $\left\{\frac{\varepsilon_2, \mu}{\mathfrak{l}_{t-1}}\right\} = \zeta$. Wir betrachten nunmehr alle diejenigen Einheiten ξ_3, für welche sowohl $\left\{\frac{\xi_3, \mu}{\mathfrak{l}_t}\right\} = 1$ als auch $\left\{\frac{\xi_3, \mu}{\mathfrak{l}_{t-1}}\right\} = 1$ wird, und sehen nach, ob unter diesen eine Einheit $\xi_3 = \varepsilon_3$ vorhanden ist, für welche

wenigstens eines der $t-2$ Symbole

$$\left\{\frac{\varepsilon_3,\ \mu}{\mathfrak{l}_1}\right\},\quad \ldots,\quad \left\{\frac{\varepsilon_3,\ \mu}{\mathfrak{l}_{t-2}}\right\}$$

von 1 verschieden ausfällt. Fahren wir in der geeigneten Weise fort, so erhalten wir schliesslich eine gewisse Anzahl r^* und dazu ein System von r^* Einheiten $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r^*}$ des Körpers $k(\zeta)$ von der Art, dass bei geeigneter Anordnung der Primideale $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$ die Gleichungen

$$(140.)\quad \begin{cases} \left\{\frac{\varepsilon_1,\ \mu}{\mathfrak{l}_t}\right\}=\zeta, \\ \left\{\frac{\varepsilon_2,\ \mu}{\mathfrak{l}_t}\right\}=1,\ \left\{\frac{\varepsilon_2,\ \mu}{\mathfrak{l}_{t-1}}\right\}=\zeta, \\ \left\{\frac{\varepsilon_3,\ \mu}{\mathfrak{l}_t}\right\}=1,\ \left\{\frac{\varepsilon_3,\ \mu}{\mathfrak{l}_{t-1}}\right\}=1,\ \left\{\frac{\varepsilon_3,\ \mu}{\mathfrak{l}_{t-2}}\right\}=\zeta, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \left\{\frac{\varepsilon_{r^*},\ \mu}{\mathfrak{l}_t}\right\}=1,\ \left\{\frac{\varepsilon_{r^*},\ \mu}{\mathfrak{l}_{t-1}}\right\}=1,\ \left\{\frac{\varepsilon_{r^*},\ \mu}{\mathfrak{l}_{t-2}}\right\}=1,\ \ldots,\left\{\frac{\varepsilon_{r^*},\ \mu}{\mathfrak{l}_{t-r^*+1}}\right\}=\zeta \end{cases}$$

gelten, und dass ausserdem für eine jede solche Einheit ξ, die den r^* Gleichungen

$$\left\{\frac{\xi,\ \mu}{\mathfrak{l}_t}\right\}=1,\quad \left\{\frac{\xi,\ \mu}{\mathfrak{l}_{t-1}}\right\}=1,\quad \ldots,\quad \left\{\frac{\xi,\ \mu}{\mathfrak{l}_{t-r^*+1}}\right\}=1$$

genügt, notwendig auch die $r=t-r^*$ Symbole

$$\left\{\frac{\xi,\ \mu}{\mathfrak{l}_1}\right\},\quad \ldots,\quad \left\{\frac{\xi,\ \mu}{\mathfrak{l}_r}\right\}$$

sämtlich den Wert 1 besitzen.

Wir multipliciren nunmehr die vorhin aus dem Ideal $\mathfrak{J}$ gebildete Zahl ν des Körpers $k(\zeta)$ derart mit Potenzen der Einheiten $\varepsilon_1, \ldots, \varepsilon_{r^*}$, dass das entstehende Product $\bar{\nu}$ den Gleichungen

$$\left\{\frac{\bar{\nu},\ \mu}{\mathfrak{l}_t}\right\}=1,\quad \left\{\frac{\bar{\nu},\ \mu}{\mathfrak{l}_{t-1}}\right\}=1,\quad \ldots,\quad \left\{\frac{\bar{\nu},\ \mu}{\mathfrak{l}_{t-r^*+1}}\right\}=1$$

genügt; dann bezeichne ich die $r=t-r^*$ Einheiten

$$\chi_1(\mathfrak{J})=\left\{\frac{\bar{\nu},\ \mu}{\mathfrak{l}_1}\right\},\quad \ldots,\quad \chi_r(\mathfrak{J})=\left\{\frac{\bar{\nu},\ \mu}{\mathfrak{l}_r}\right\}$$

als das **Charakterensystem des Ideals** $\mathfrak{J}$. Dasselbe ist durch das Ideal $\mathfrak{J}$ völlig eindeutig bestimmt. In § 151 wird gezeigt werden, dass stets $r^* < t$ und mithin $r \geqq 1$ wird.

§ 150.

Das Charakterensystem einer Idealklasse und der Begriff des Geschlechtes.

Mit Rücksicht auf den Satz 151 und die dazu auf S. 423 angefügten Bemerkungen erkennen wir sofort die Thatsache:

Satz 160. Die Ideale ein und derselben Klasse eines regulären Kummer'schen Körpers besitzen sämtlich dasselbe Charakterensystem.

Auf diese Weise ist überhaupt einer jeden Idealklasse ein bestimmtes Charakterensystem zuzuordnen. Wir rechnen, ähnlich wie es in § 66 für den quadratischen Körper geschehen ist, alle diejenigen Idealklassen, welche ein und dasselbe Charakterensystem besitzen, in ein **Geschlecht** und definiren insbesondere das **Hauptgeschlecht** als die Gesamtheit aller derjenigen Klassen, deren Charakterensystem aus lauter Einheiten 1 besteht. Da das Charakterensystem der Hauptklasse offenbar von der letzteren Eigenschaft ist, so gehört insbesondere die Hauptklasse stets zum Hauptgeschlecht. Aus der ersten Formel in (80.) und in (83.) auf S. 411 und S. 413 entnehmen wir leicht die folgenden Thatsachen: Wenn G und G' zwei beliebige Geschlechter sind und jede Klasse in G mit jeder Klasse in G' multiplicirt wird, so bilden sämtliche solche Producte wiederum ein Geschlecht; dieses werde das **Product der Geschlechter** G und G' genannt. Das Charakterensystem desselben erhalten wir durch Multiplication der entsprechenden Charaktere der beiden Geschlechter G und G'.

Aus der eben aufgestellten Definition der Geschlechter leuchtet ferner ein, dass die zu einer Klasse C relativ conjugirten Klassen $SC, \ldots, S^{l-1}C$ zu demselben Geschlechte wie C selbst gehören, und hieraus folgt, dass die $(1-S)$te symbolische Potenz C^{1-S} einer jeden Klasse C stets zum Hauptgeschlecht gehört. Endlich ist offenbar, dass jedes Geschlecht des Kummer'schen Körpers gleich viel Klassen enthält.

§ 151.

Obere Grenze für den Grad der aus sämtlichen ambigen Klassen bestehenden Klassenschar.

Es entsteht, entsprechend wie in der Theorie des quadratischen Körpers, die wichtige Frage, ob ein System von r beliebig vorgelegten

$l$ten Einheitswurzeln stets das Charakterensystem für ein Geschlecht des Kummer'schen Körpers sein kann. Diese Frage findet erst in Capitel XXXIV ihre vollständige Erledigung. In diesem und in den nächsten Paragraphen werden lediglich einige für das Spätere notwendige Hülfssätze bewiesen.

Hülfssatz 33. Wenn t und n die Bedeutung wie in Satz 159 haben und r die Anzahl der Charaktere ist, welche das Geschlecht einer Klasse des Kummer'schen Körpers bestimmen, so ist stets

$$t+n-\frac{l+1}{2} \leqq r-1.$$

Beweis. Es seien $\varepsilon_1, \ldots, \varepsilon_{r^*}$ diejenigen besonderen r^* Einheiten des Körpers $k(\zeta)$, welche in § 149 eingeführt worden sind. Es ist dann $r=t-r^*$. Ferner mögen $\vartheta_1, \ldots, \vartheta_n$ eine Basis für diejenige Einheitenschar in $k(\zeta)$ bilden, welche aus allen Einheiten in $k(\zeta)$ besteht, die Relativnormen von Zahlen in K sind. Wir nehmen nun an, es gäbe zwischen den r^*+n Einheiten $\varepsilon_1, \ldots, \varepsilon_{r^*}, \vartheta_1, \ldots, \vartheta_n$ eine Relation von der Gestalt

$$(141.) \qquad \varepsilon_1^{a_1}\ldots\varepsilon_{r^*}^{a_{r^*}}\vartheta_1^{b_1}\ldots\vartheta_n^{b_n} = \varepsilon^l,$$

so dass die Exponenten $a_1, \ldots, a_{r^*}, b_1, \ldots, b_n$ ganze rationale, nicht sämtlich durch l teilbare Zahlen sind und ε eine geeignete Einheit in $k(\zeta)$ vorstellt; dann müsste für $u=1, 2, \ldots, t$ stets

$$\left\{\frac{\varepsilon_1^{a_1}\ldots\varepsilon_{r^*}^{a_{r^*}}\vartheta_1^{b_1}\ldots\vartheta_n^{b_n},\ \mu}{\mathfrak{l}_u}\right\} = 1$$

ausfallen, und wenn wir berücksichtigen, dass die Einheiten $\vartheta_1, \ldots, \vartheta_n$ sämtlich Relativnormen von Zahlen in K sind und daher stets $\left\{\frac{\vartheta_v,\ \mu}{\mathfrak{l}_u}\right\}=1$ für $u=1, 2, \ldots, t$ und $v=1, 2, \ldots, n$ sein muss, so ergiebt sich auch

$$\left\{\frac{\varepsilon_1^{a_1}\ldots\varepsilon_{r^*}^{a_{r^*}},\ \mu}{\mathfrak{l}_u}\right\} = 1$$

für $u=1, 2, \ldots, t$. Wegen der Formeln (140.) für die Einheiten $\varepsilon_1, \ldots, \varepsilon_{r^*}$ ist dies nur möglich, wenn die Exponenten $a_1, \ldots, a_{r^*}$ sämtlich durch l teilbar sind, und die Relation (141.) würde somit die Gestalt

$$\vartheta_1^{b_1}\ldots\vartheta_n^{b_n} = \varepsilon^{*l}$$

annehmen, wo ε^* wiederum eine Einheit in $k(\zeta)$ bedeutet. Das Bestehen einer solchen Relation ist aber, da $\vartheta_1, \ldots, \vartheta_n$ die Basis einer Einheitenschar in $k(\zeta)$ bilden, nur möglich, falls die Exponenten $b_1, \ldots, b_n$ sämtlich durch l teilbar sind. Daraus folgt, dass eine Relation von der Gestalt (141.), wie wir sie annahmen, nicht statthaben kann, d. h. die Einheiten $\varepsilon_1, \ldots, \varepsilon_{r^*}, \vartheta_1, \ldots, \vartheta_n$ bilden eine Basis einer Einheitenschar; es ist der Grad dieser Einheitenschar r^*+n, und da der Grad einer Einheitenschar höchstens $\frac{l-1}{2}$ sein kann, so haben wir $r^*+n \leqq \frac{l-1}{2}$; hiermit deckt sich die Aussage des Hülfssatzes 33. Da $t+n-\frac{l+1}{2} \geqq 0$ ist, so folgt insbesondere, dass stets $r^* < t$, also $r \geqq 1$ ausfällt.

§ 152.

Die Complexe des regulären Kummer'schen Körpers.

Es sei h die Anzahl der Idealklassen des regulären Kreiskörpers $k(\zeta)$: dann giebt es in dem Kummer'schen Körper $K = k(\sqrt[l]{\mu}, \zeta)$ genau h von einander verschiedene Idealklassen, welche unter ihren Idealen Ideale des Kreiskörpers $k(\zeta)$ enthalten. In der That, jede Klasse in $k(\zeta)$ liefert offenbar eine Klasse in K von der fraglichen Art; würden nun zwei verschiedene Klassen c_1, c_2 in $k(\zeta)$ Ideale enthalten, die in K einander äquivalent sind, so würde ein Ideal $\mathfrak{j}$ in $k(\zeta)$ aus der Klasse $\frac{c_1}{c_2}$ stets zu einem Hauptideal im Körper K werden müssen. Nach Satz 153 wäre dann aber $\mathfrak{j}$ auch ein Hauptideal in $k(\zeta)$, und dies ist gegen die Annahme $c_1 \neq c_2$.

Ist nun C eine beliebige Klasse in K und sind $c_1, \ldots, c_h$ diejenigen h Klassen in K, welche Ideale in $k(\zeta)$ enthalten, so nenne ich das System der h Klassen $c_1 C, \ldots, c_h C$ einen **Complex.** Der Complex, welcher aus den h Klassen $c_1, \ldots, c_h$ besteht, heisse der **Hauptcomplex** und werde mit 1 bezeichnet. Die h Klassen eines beliebigen Complexes P gehören offenbar sämtlich zu dem nämlichen Geschlecht; ich bezeichne dieses Geschlecht als das **Geschlecht des Complexes** P.

Wenn eine Klasse eines Complexes P ambig ist, so sind sämtliche Klassen dieses Complexes ambig; den Complex P nenne ich dann einen **ambigen Complex.**

Wenn P und P' zwei beliebige Complexe sind und jede Klasse in

P mit jeder Klasse in P' multiplicirt wird, so bilden sämtliche solche Producte wiederum einen Complex; dieser werde das **Product der Complexe** P, P' genannt und mit PP' bezeichnet. Wenn C eine Klasse in P ist, so werde derjenige Complex, zu welchem die relativ conjugirte Klasse SC gehört, mit SP bezeichnet; ferner nenne ich denjenigen Complex Q, der nach der Multiplication mit SP den Complex P ergiebt, die **symbolische** $(1-S)$**te Potenz des Complexes** P und bezeichne ihn mit $Q = P^{1-S}$.

Wenn insbesondere die symbolische $(1-S)$te Potenz eines Complexes P den Hauptcomplex 1 liefert, so ist P ein ambiger Complex. In der That, wenn C eine Klasse in P ist, so folgt aus $P^{1-S} = 1$ offenbar $C^{1-S} = c$, wo c eine der h Idealklassen $c_1, \ldots, c_h$ ist. Bilden wir auf beiden Seiten der letzten Gleichung die Relativnorm, so erhalten wir $1 = c^l$, und da andererseits auch $c^h = 1$ ist, so folgt $c = 1$, d. h. $C^{1-S} = 1$; mithin ist C eine ambige Klasse und daher P ein ambiger Complex.

§ 153.

Obere Grenze für die Anzahl der Geschlechter in einem regulären Kummer'schen Körper.

Hülfssatz 34. Wenn t und n die Bedeutung wie in Satz 159 haben und g die Anzahl der Geschlechter des regulären Kummer'schen Körpers K bezeichnet, so fällt stets $g \leqq l^{t+n-\frac{l+1}{2}}$ aus.

Beweis. Wenn g die Anzahl der Geschlechter in dem Kummer'schen Körper K ist, so zerfallen, wie man unmittelbar aus der Definition des Geschlechtes eines Complexes ersieht, auch die Complexe genau in g Geschlechter. Bezeichnen wir daher mit f die Anzahl der Complexe vom Hauptgeschlecht, so ist die Anzahl aller überhaupt vorhandenen Complexe, welche M heisse, genau $M = fg$.

Wir wollen nun die Anzahl a der ambigen Complexe ermitteln. Zu dem Zwecke bedenken wir, dass nach Satz 159 der Grad der aus allen ambigen Klassen bestehenden Klassenschar gleich $t+n-\dfrac{l+1}{2}$ ist. Es sei $A_1, \ldots, A_{t+n-\frac{l+1}{2}}$ eine Basis dieser Klassenschar, dann stellt der Ausdruck

$$A_1^{u_1} \ldots A_{t+n-\frac{l+1}{2}}^{u_{t+n-\frac{l+1}{2}}},$$

wenn die Exponenten $u_1, \ldots, u_{t+n-\frac{l+1}{2}}$ unabhängig von einander die Werte $0, 1, \ldots, l-1$ durchlaufen, lauter ambige Klassen dar, welche in verschiedenen Complexen liegen, und es werden somit durch diese Klassen genau $l^{t+n-\frac{l+1}{2}}$ Complexe bestimmt. Jede vorhandene ambige Klasse A ist in der Gestalt

$$A = A_1^{a_1} \ldots A_{t+n-\frac{l+1}{2}}^{a_{t+n-\frac{l+1}{2}}} c$$

darstellbar, wo $a_1, \ldots, a_{t+n-\frac{l+1}{2}}$ ganze rationale Exponenten sind und c eine Klasse in $k(\zeta)$ bedeutet. Berücksichtigen wir nun, dass die $l$ten Potenzen der ambigen Klassen $A_1, \ldots, A_{t+n-\frac{l+1}{2}}$ Klassen sind, welche Ideale des Körpers $k(\zeta)$ enthalten, so folgt, dass A notwendig einem der oben bestimmten $l^{t+n-\frac{l+1}{2}}$ Complexe angehören muss, und mithin ist die gesuchte Anzahl $a = l^{t+n-\frac{l+1}{2}}$.

Aus den Definitionen in § 150 und § 152 geht unmittelbar hervor, dass die symbolische $(1-S)$te Potenz eines beliebigen Complexes stets ein Complex des Hauptgeschlechtes ist. Wir fassen nun diejenigen Complexe des Hauptgeschlechtes ins Auge, welche $(1-S)$te symbolische Potenzen von Complexen sind; ihre Anzahl sei f'; wir bezeichnen sie mit $P_1, \ldots, P_{f'}$, und wir mögen $P_1 = G_1^{1-S}, \ldots, P_{f'} = G_{f'}^{1-S}$ haben, wo $G_1, \ldots, G_{f'}$ gewisse Complexe bedeuten. Ist jetzt P ein beliebiger Complex, so ist P^{1-S} notwendig ein bestimmter der f' Complexe $P_1, \ldots, P_{f'}$; es sei etwa $P^{1-S} = P_v$. Dann folgt $P^{1-S} = G_v^{1-S}$, d. h. $(PG_v^{-1})^{1-S} = 1$, und somit ist PG_v^{-1} ein bestimmter ambiger Complex A; es wird $P = AG_v$, und folglich stellt der Ausdruck AG_v alle Complexe dar, sobald A alle ambigen Complexe und G_v die f' Complexe $G_1, \ldots, G_{f'}$ durchläuft. Auch ist klar, dass diese Darstellung für jeden Complex nur auf eine Weise möglich ist; es ist daher die Anzahl aller überhaupt vorhandenen Complexe $M = af'$. Die Zusammenstellung dieser Gleichung mit der vorhin gefundenen $M = gf$ liefert $af' = gf$, und wegen $f' \leqq f$ folgt hieraus $g \leqq a$, d. h. $g \leqq l^{t+n-\frac{l+1}{2}}$, und hiermit ist der Hülfssatz 34 bewiesen.

Aus den beiden Hülfssätzen 33 und 34 folgt sofort die weitere Thatsache:

Hülfssatz 35. Wenn in einem regulären Kummer'schen Körper r die Anzahl der Charaktere ist, welche das Geschlecht einer Klasse bestimmen, so ist die Anzahl der Geschlechter jenes Körpers $g \leqq l^{r-1}$.

Capitel XXXIII.

Das Reciprocitätsgesetz für $l$te Potenzreste im regulären Kreiskörper.

§ 154.

Das Reciprocitätsgesetz für $l$te Potenzreste und die Ergänzungssätze.

Die bisher dargelegte Theorie des Kummer'schen Körpers liefert uns die Hülfsmittel zum Beweise gewisser fundamentaler Gesetze über $l$te Potenzreste im regulären Kreiskörper, welche den Reciprocitätsgesetzen für quadratische Reste im Gebiete der rationalen Zahlen entsprechen, und welche das in § 115 entwickelte *Eisenstein*'sche Reciprocitätsgesetz (Satz 140) zwischen einer beliebigen Zahl in $k(\zeta)$ und einer rationalen Zahl als besonderen Fall enthalten. Um diese Gesetze für $l$te Potenzreste in ihrer einfachsten Gestalt aussprechen zu können, verallgemeinern wir das in § 113 und § 127 definirte Symbol $\left\{\frac{\mu}{\mathfrak{w}}\right\}$ in folgender Weise:

Es sei h die Anzahl der Idealklassen in $k(\zeta)$; dann bestimmen wir eine ganze rationale positive Zahl h^* so, dass $hh^* \equiv 1$ nach l wird. Bedeutet dann $\mathfrak{p}$ ein beliebiges, von $\mathfrak{l}$ verschiedenes Primideal in $k(\zeta)$, so ist stets $\mathfrak{p}^{hh^*}$ ein Hauptideal in $k(\zeta)$; wir setzen $\mathfrak{p}^{hh^*} = (\pi)$, so dass π eine ganze Zahl in $k(\zeta)$ ist, und nehmen hierin, was dem Satze 157 zufolge geschehen kann, die Zahl π primär an. Eine solche ganze Zahl π heisse eine **Primärzahl von** $\mathfrak{p}$. Es hat dann, da jede primäre Einheit in $k(\zeta)$ zufolge einer Bemerkung auf S. 441 die $l$te Potenz einer Einheit in $k(\zeta)$ ist, π in Bezug auf jedes von $\mathfrak{p}$ verschiedene Primideal einen völlig bestimmten Potenzcharakter. Bedeutet nun $\mathfrak{q}$ ein beliebiges, von $\mathfrak{l}$ und von $\mathfrak{p}$ verschiedenes Primideal in $k(\zeta)$, so wird das

Symbol $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}$ durch die Formel

$$\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = \left\{\frac{\pi}{\mathfrak{q}}\right\}$$

definirt. Das Symbol $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}$ ist somit eine durch die zwei Primideale $\mathfrak{p}$ und $\mathfrak{q}$ eindeutig bestimmte $l$te Einheitswurzel. Mit Benutzung dieses Symbols sprechen wir folgende Thatsache aus:

Satz 161. *Sind* $\mathfrak{p}$ *und* $\mathfrak{q}$ *von einander und von dem Primideal* $\mathfrak{l}$ *verschiedene Primideale des regulären* ***K****reiskörpers* $k(\zeta)$, *so gilt die Regel*

$$\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\},$$

das sogenannte Reciprocitätsgesetz für lte Potenzreste. Ausserdem gelten, wenn ξ *eine beliebige Einheit in* $k(\zeta)$ *und* π *eine Primärzahl von dem Primideal* $\mathfrak{p}$ *bedeutet, die Regeln*

$$\left\{\frac{\xi}{\mathfrak{p}}\right\} = \left\{\frac{\pi,\ \xi}{\mathfrak{l}}\right\},\quad \left\{\frac{\lambda}{\mathfrak{p}}\right\} = \left\{\frac{\pi,\ \lambda}{\mathfrak{l}}\right\},$$

die beiden sogenannten Ergänzungssätze zum Reciprocitätsgesetz für l*te Potenzreste.* [*Kummer*[10, 12, 18, 19, 20, 21].]

Wir führen den Nachweis dieses Fundamentalsatzes in den folgenden Paragraphen § 155 — § 161 des gegenwärtigen Capitels durch schrittweises Vorgehen, indem wir für besondere reguläre Kummer'sche Körper die im vorigen Capitel gefundenen Sätze und Hülfssätze zur Anwendung bringen.

§ 155.

Die Primideale erster und zweiter Art im regulären Kreiskörper.

Es ist für die folgenden Entwickelungen von Nutzen, zwei Arten von Primidealen in $k(\zeta)$ zu unterscheiden: ein solches von $\mathfrak{l}$ verschiedenes Primideal $\mathfrak{p}$ in $k(\zeta)$, nach welchem nicht jede vorhandene Einheit in $k(\zeta)$ $l$ter Potenzrest ist, möge ein **Primideal erster Art** heissen; dagegen möge jedes von $\mathfrak{l}$ verschiedene Primideal $\mathfrak{q}$ in $k(\zeta)$, nach welchem alle Einheiten in $k(\zeta)$ $l$te Potenzreste sind, ein **Primideal zweiter Art** heissen. [*Kummer*[20].] Wir beweisen zunächst folgende Hülfssätze:

Hülfssatz 36. Wenn ξ und ε beliebige Einheiten des regulären

Kreiskörpers $k(\zeta)$ sind und $\lambda = 1 - \zeta$, $\mathfrak{l} = (\lambda)$ gesetzt wird, so gelten stets die Gleichungen

$$\left\{\frac{\xi,\ \varepsilon}{\mathfrak{l}}\right\} = 1, \quad \left\{\frac{\lambda,\ \varepsilon}{\mathfrak{l}}\right\} = 1.$$

Beweis. Wenn ε die $l$te Potenz einer Einheit in $k(\zeta)$ ist, so leuchtet die Richtigkeit der aufgestellten Gleichungen von selbst ein. Anderen Falles definirt $\sqrt[l]{\varepsilon}$ einen Kummer'schen Körper $k(\sqrt[l]{\varepsilon}, \zeta)$, und zwar einen solchen, für welchen die Betrachtungen am Schluss des § 147 zutreffen. Es sind daher alle Einheiten in $k(\zeta)$ und zudem auch die Zahl λ Relativnormen von Zahlen in $k(\sqrt[l]{\varepsilon}, \zeta)$, und hieraus ergiebt sich wegen Satz 151 die Richtigkeit der Gleichungen des Hülfssatzes 36.

Will man hier den Satz 151 für $\mathfrak{w} = \mathfrak{l}$ nur in dem auf S. 422 — S. 423 ausführlich behandelten Fall anwenden, wo die betreffende Zahl $\mu \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ ist, so mache man die letzten Schlüsse zunächst, indem man ζ^{l-1} für die Einheit ε nimmt; dann folgt $\left\{\frac{\xi,\ \zeta}{\mathfrak{l}}\right\} = 1$ und $\left\{\frac{\lambda,\ \zeta}{\mathfrak{l}}\right\} = 1$. Weiter bestimme man, wenn ε eine beliebige Einheit in $k(\zeta)$ bedeutet, eine solche $l$te Einheitswurzel ζ^*, dass $\zeta^* \varepsilon^{l-1} \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ ausfällt. Nimmt man dann im oben dargelegten Beweise $\zeta^* \varepsilon^{l-1}$ an Stelle der Einheit ε, so folgt unter Benutzung der zweiten Formel in (83.) (S. 413) $\left\{\frac{\xi,\ \varepsilon}{\mathfrak{l}}\right\} = 1$ und in gleicher Weise $\left\{\frac{\lambda,\ \varepsilon}{\mathfrak{l}}\right\} = 1$.

Hülfssatz 37. Wenn $\mathfrak{p}$ ein Primideal erster Art und π eine Primärzahl von $\mathfrak{p}$ ist, so giebt es in $k(\zeta)$ stets wenigstens eine Einheit ε, für welche

$$\left\{\frac{\varepsilon,\ \pi}{\mathfrak{l}}\right\} \neq 1$$

ausfällt; ist dagegen ein Primideal $\mathfrak{q}$ zweiter Art vorgelegt und bedeutet $\varkappa$ eine Primärzahl von $\mathfrak{q}$, so gilt für jede Einheit ξ in $k(\zeta)$ die Gleichung

$$\left\{\frac{\xi,\ \varkappa}{\mathfrak{l}}\right\} = 1.$$

Beweis. Um die erste Aussage dieses Hülfssatzes zu beweisen, nehmen wir an, es gelte im Gegenteil für jede Einheit ξ in $k(\zeta)$ die

Gleichung

$$\left\{\frac{\xi,\ \pi}{\mathfrak{l}}\right\} = 1.$$

Wir setzen $\pi \equiv a + b\lambda^e$ nach $\mathfrak{l}^{e+1}$, wobei a und b ganze rationale Zahlen sein sollen und e den grössten Exponent $\leqq l-1$ bedeutet, für den jener Ansatz möglich ist Da π eine primäre Zahl ist, so muss notwendig $e > 1$ und $\pi . s^{\frac{l-1}{2}} \pi$ einer ganzen rationalen Zahl nach l congruent sein; hierbei bedeutet $s^{\frac{l-1}{2}}$ die Substitution $(\zeta : \zeta^{-1})$ aus der Gruppe des Kreiskörpers $k(\zeta)$. Da $s^{\frac{l-1}{2}} \lambda \equiv -\lambda$ nach $\mathfrak{l}^2$ ist, so wird

$$\pi . s^{\frac{l-1}{2}} \pi \equiv (a + b\lambda^e)(a + b(-\lambda)^e), \quad (\mathfrak{l}^{e+1}),$$

und hieraus folgt, dass im Falle $e < l-1$ der Exponent e notwendig ungerade sein muss.

Wir haben nun beim Beweise des Hülfssatzes 29 gefunden, dass die $l^* = \frac{l-3}{2}$ dort mit $\varepsilon_1, \ldots, \varepsilon_{l^*}$ bezeichneten Einheiten des Kreiskörpers $k(\zeta)$ die Bedingungen

$$\left.\begin{array}{l} \mathrm{l}^{(u)}(\varepsilon_t) \equiv 0, \quad (l), \quad (u \neq 2t) \\ \mathrm{l}^{(2t)}(\varepsilon_t) \not\equiv 0, \quad (l) \end{array}\right\} \qquad \left(\begin{array}{l} t = 1, 2, \ldots, l^*; \\ u = 1, 2, \ldots, l-2 \end{array}\right)$$

erfüllen. Setzen wir in der Gleichung oben auf dieser Seite der Reihe nach für ξ die Werte $\varepsilon_1, \ldots, \varepsilon_{l^*}$ ein, so entspringen zufolge der Definition (82.) des Symbols $\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\}$ auf S. 413 und ihrer auf S. 414 gegebenen Ausdehnung die Congruenzen

$$\mathrm{l}^{(l-2)}(\pi^{l-1}) \equiv 0,\ \mathrm{l}^{(l-4)}(\pi^{l-1}) \equiv 0,\ \mathrm{l}^{(l-6)}(\pi^{l-1}) \equiv 0, \ldots, \mathrm{l}^{(3)}(\pi^{l-1}) \equiv 0,\ (l);$$

und diese lassen erkennen, dass in der Congruenz $\pi \equiv a + b\lambda^e$ nach $\mathfrak{l}^{e+1}$ der Exponent e keinen der Werte $l-2,\ l-4,\ l-6, \ldots, 3$ haben darf. Stellen wir damit die oben gefundenen Bedingungen für e zusammen, so folgt, dass $e = l-1$ sein muss. Da nun $\lambda^{l-1} \equiv -l$ nach $\mathfrak{l}^l$ wird, so ergiebt sich $\pi \equiv a - bl$ nach $\mathfrak{l}^l$, und folglich genügt die Norm von π der Congruenz

$$n(\pi) \equiv (a - bl)^{l-1} \equiv \pi^{l-1}, \quad (\mathfrak{l}^l).$$

Andererseits entnehmen wir aus der Definition des Symbols auf S. 413

und S. 414 unter Berücksichtigung des Hülfssatzes 24

$$\left\{\frac{\zeta,\,\pi}{\mathfrak{l}}\right\} = \zeta^{\frac{1-n(\pi)}{l}},$$

und da das Symbol linker Hand den Wert 1 haben soll, so folgt $n(\pi) \equiv 1$ nach l^2, d. h. $\pi^{l-1} \equiv 1$ nach $\mathfrak{l}^l$ oder $\pi \equiv \pi^l$ nach $\mathfrak{l}^l$. Nach Satz 148 besitzt infolge der letzteren Congruenz der durch $\sqrt[l]{\pi}$ bestimmte Kummer'sche Körper $k(\sqrt[l]{\pi}, \zeta)$ eine zu $\mathfrak{l}$ prime Relativdiscriminante, und es ist mithin $\mathfrak{p}$ das einzige in der Relativdiscriminante von $k(\sqrt[l]{\pi}, \zeta)$ aufgehende Primideal. Setzen wir $\mathfrak{p} = \mathfrak{P}^l$, so ist $\mathfrak{P}$ das einzige ambige Primideal dieses Körpers. Aus $\sqrt[l]{\pi} = \mathfrak{P}^{hh^*} = \mathfrak{P}\mathfrak{p}^{\frac{hh^*-1}{l}}$ folgt, dass $\mathfrak{P}$ einem Ideal des Körpers $k(\zeta)$ äquivalent ist. Die aus allen ambigen Idealen entspringende Klassenschar hat also für den Kummer'schen Körper $k(\sqrt[l]{\pi}, \zeta)$ den Grad 0. Da die Anzahl t der ambigen Ideale für diesen Körper 1 ist, so folgt nach Satz 158, wenn m die dort festgesetzte Bedeutung für diesen Körper hat, $1 + m - \frac{l+1}{2} = 0$, d. h. $m = \frac{l-1}{2}$. Es ist folglich jede Einheit ξ in $k(\zeta)$ die Relativnorm einer Einheit in $k(\sqrt[l]{\pi}, \zeta)$, und mithin wird nach Satz 151 stets $\left\{\frac{\xi,\,\pi}{\mathfrak{p}}\right\} = 1$ und also, da $\left\{\frac{\xi,\,\pi}{\mathfrak{p}}\right\} = \left\{\frac{\xi^{hh^*}}{\mathfrak{p}}\right\} = \left\{\frac{\xi}{\mathfrak{p}}\right\}$ ist, auch $\left\{\frac{\xi}{\mathfrak{p}}\right\} = 1$, entgegen unserer Annahme, wonach das Primideal $\mathfrak{p}$ von der ersten Art sein sollte.

Um die zweite Aussage des Hülfssatzes 37 zu beweisen, betrachten wir ähnlich wie im Beweise des Hülfssatzes 36 den Kummer'schen Körper $k(\sqrt[l]{\xi}, \zeta)$, wo ξ eine beliebige Einheit in $k(\zeta)$, nur nicht die $l$te Potenz einer Einheit in $k(\zeta)$, sein soll. Wie am Schlusse des § 147 bewiesen wurde, ist jede Einheit in $k(\zeta)$ die Relativnorm einer Einheit in $k(\sqrt[l]{\xi}, \zeta)$ und daher haben die beiden in Satz 158 und in Satz 159 bezeichneten Einheitenscharen für diesen Körper den gemeinsamen Grad

$$m = n = \frac{l-1}{2}.$$

Da ferner für ihn $t = 1$ ist, so folgt aus Hülfssatz 34 $g \leqq 1$; mithin

ist $g=1$, d. h. alle Idealklassen des Körpers $k(\sqrt[l]{\xi}, \zeta)$ gehören zum Hauptgeschlecht. Da $\mathfrak{q}$ ein Primideal zweiter Art sein soll, so ist $\left\{\frac{\xi}{\mathfrak{q}}\right\}=1$, und mithin zerfällt nach Satz 149 $\mathfrak{q}$ in l von einander verschiedene Primideale des Körpers $k(\sqrt[l]{\xi}, \zeta)$; es sei $\mathfrak{Q}$ einer dieser Primfactoren von $\mathfrak{q}$. Das Charakterensystem einer Zahl α $(\neq 0)$ des Körpers $k(\zeta)$ in $k(\sqrt[l]{\xi}, \zeta)$ besteht aus dem einen Charakter $\left\{\frac{\alpha, \xi}{\mathfrak{l}}\right\}$; derselbe fällt nach Hülfssatz 36 stets gleich 1 aus, wenn man für α eine Einheit in $k(\zeta)$ nimmt. Der Charakter des Primideals $\mathfrak{Q}$ in $k(\sqrt[l]{\xi}, \zeta)$ hat daher den Wert $\left\{\frac{\varkappa, \xi}{\mathfrak{l}}\right\}$, und dieser muss wegen der vorhin bewiesenen Thatsache gleich 1 sein. Damit ist der Hülfssatz 37 vollständig bewiesen.

Will man wiederum Satz 151 für $\mathfrak{w}=\mathfrak{l}$ nur in dem Falle eines Körpers $k(\sqrt[l]{\mu}, \zeta)$, für den $\mu \equiv 1+\lambda$ nach $\mathfrak{l}^2$ ist, als bewiesen annehmen, so gilt auch die Einteilung der Geschlechter und insbesondere der Hülfssatz 34 nur für diesen Fall. Wir müssen dann zum Beweise der zweiten Aussage des Hülfssatzes 37 erst $\xi=\zeta^{l-1}$ und dann $\xi=\zeta^* \varepsilon^{l-1}$ wählen, wobei ε eine beliebige Einheit in $k(\zeta)$ und ζ^* dazu eine solche $l$te Einheitswurzel bedeute, dass $\zeta^* \varepsilon^{l-1} \equiv 1+\lambda$ nach $\mathfrak{l}^2$ wird. Durch Verbindung der beiden sich dabei ergebenden Resultate erkennen wir dann die vollständige Richtigkeit der zweiten Aussage des Hülfssatzes 37.

§ 156.

Hülfssätze über Primideale erster Art im regulären Kreiskörper.

Wir beweisen der Reihe nach folgende Hülfssätze über Primideale erster Art im Körper $k(\zeta)$:

Hülfssatz 38. Es sei $\mathfrak{p}$ ein Primideal erster Art im regulären Kreiskörper $k(\zeta)$ und π eine Primärzahl von $\mathfrak{p}$. Wenn es dann eine Einheit ε in $k(\zeta)$ giebt, so dass

$$\left\{\frac{\pi, \varepsilon}{\mathfrak{l}}\right\} \neq 1, \quad \left\{\frac{\varepsilon}{\mathfrak{p}}\right\}=\left\{\frac{\pi, \varepsilon}{\mathfrak{l}}\right\}$$

statthat, so gilt für jede beliebige Einheit ξ in $k(\zeta)$ die Gleichung:

$$\left\{\frac{\xi}{\mathfrak{p}}\right\}=\left\{\frac{\pi, \xi}{\mathfrak{l}}\right\}.$$

Beweis. Der durch $\sqrt[l]{\pi}$ bestimmte Kummer'sche Körper $k(\sqrt[l]{\pi}, \zeta)$ besitzt, weil $\mathfrak{p}$ ein Primideal erster Art ist, nach dem Beweise des Hülfssatzes 37 zwei ambige Primideale $\mathfrak{L}$ und $\mathfrak{P}$, nämlich diejenigen, deren $l$te Potenzen $\mathfrak{l}$ bez. $\mathfrak{p}$ sind. Da das ambige Primideal $\mathfrak{P}$ offenbar Hauptideal in $k(\sqrt[l]{\pi}, \zeta)$ ist, so beträgt für diesen Körper der Grad der aus den ambigen Idealen entspringenden Klassenschar 0 oder 1, je nachdem $\mathfrak{L}$ Hauptideal ist oder nicht. Wegen des Satzes 158 besitzt daher, wenn m die dort erklärte Bedeutung für den Körper $k(\sqrt[l]{\pi}, \zeta)$ hat, die Zahl $2 + m - \frac{l+1}{2}$ den Wert 0 der 1, d. h. es ist $m = \frac{l-3}{2}$ oder $m = \frac{l-1}{2}\cdot$ Da die Einheit ε infolge der Voraussetzung $\left\{\frac{\varepsilon, \pi}{\mathfrak{l}}\right\} \neq 1$ mit Rücksicht auf Satz 151 sicher nicht die Relativnorm einer Einheit des Körpers $k(\sqrt[l]{\pi}, \zeta)$ ist, so haben wir notwendigerweise $m = \frac{l-3}{2}$, und es ist sodann jede Einheit ξ in $k(\zeta)$ in der Gestalt $\xi = \varepsilon^a \vartheta$ darstellbar, wo a ein ganzer rationaler Exponent und ϑ eine solche Einheit bedeutet, die sich als Relativnorm einer Einheit in $k(\sqrt[l]{\pi}, \zeta)$ erweist. Aus dem letzteren Grunde ist wegen Satz 151

$$\left\{\frac{\vartheta,\ \pi}{\mathfrak{l}}\right\} = 1, \quad \left\{\frac{\vartheta,\ \pi}{\mathfrak{p}}\right\} = \left\{\frac{\vartheta}{\mathfrak{p}}\right\} = 1$$

und also auch $\left\{\frac{\pi, \vartheta}{\mathfrak{l}}\right\} = \left\{\frac{\vartheta}{\mathfrak{p}}\right\}$; hieraus folgt unter Benutzung der zweiten Formel in (83.) (S. 413) auch $\left\{\frac{\pi, \xi}{\mathfrak{l}}\right\} = \left\{\frac{\xi}{\mathfrak{p}}\right\}$, und damit ist der Beweis für den Hülfssatz 38 erbracht.

Soll Satz 151 für $\mathfrak{w} = \mathfrak{l}$ nur in dem Falle eines Körpers $k(\sqrt[l]{\mu}, \zeta)$, für den $\mu \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ ist, angewandt werden, so bestimme man eine $l$te Einheitswurzel ζ^* derart, dass $\zeta^* \pi^{l-1} \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ wird, und dann betrachte man, indem man im Uebrigen wie in dem oben dargelegten Beweise verfährt, an Stelle des Körpers $k(\sqrt[l]{\pi}, \zeta)$ den Körper $k(\sqrt[l]{\zeta^* \pi^{l-1}}, \zeta)$. Wenn man schliesslich noch den Hülfssatz 36 zuzieht, folgt dann der Hülfssatz 38 vollständig.

Hülfssatz 39. Wenn $\mathfrak{p}$, $\mathfrak{p}^*$ zwei Primideale erster Art in $k(\zeta)$ und π, π^* Primärzahlen bez. von $\mathfrak{p}$, $\mathfrak{p}^*$ sind, wenn ferner für jede be-

liebige Einheit ξ in $k(\zeta)$

$$\left\{\frac{\xi}{\mathfrak{p}}\right\}=\left\{\frac{\pi,\ \xi}{\mathfrak{l}}\right\},\quad \left\{\frac{\xi}{\mathfrak{p}^*}\right\}=\left\{\frac{\pi^*,\ \xi}{\mathfrak{l}}\right\}$$

wird, so ist

$$\left\{\frac{\mathfrak{p}}{\mathfrak{p}^*}\right\}=\left\{\frac{\mathfrak{p}^*}{\mathfrak{p}}\right\}.$$

Beweis. Da $\mathfrak{p}^*$ ein Primideal erster Art ist, so können wir eine Einheit ε in $k(\zeta)$ derart bestimmen, dass $\left\{\frac{\varepsilon\pi}{\mathfrak{p}^*}\right\}=1$ wird. Wir betrachten nun den Kummer'schen Körper $k(\sqrt[l]{\varepsilon\pi},\zeta)$. Da die Relativdiscriminante dieses Körpers nur die beiden Primfactoren $\mathfrak{l}$ und $\mathfrak{p}$ enthält, so besteht das Charakterensystem einer Zahl α $(\neq 0)$ in $k(\zeta)$ für diesen Körper aus den zwei Charakteren $\left\{\frac{\alpha,\ \varepsilon\pi}{\mathfrak{l}}\right\}$ und $\left\{\frac{\alpha,\ \varepsilon\pi}{\mathfrak{p}}\right\}=\left\{\frac{\alpha}{\mathfrak{p}}\right\}$. Wegen $\left\{\frac{\varepsilon\pi}{\mathfrak{p}^*}\right\}=1$ ist $\mathfrak{p}^*$ in $k(\sqrt[l]{\varepsilon\pi},\zeta)$ weiter zerlegbar; es sei $\mathfrak{P}^*$ ein Primfactor von $\mathfrak{p}^*$ in diesem Körper. Um das Charakterensystem von $\mathfrak{P}^*$ zu bilden, bedenken wir, dass $\mathfrak{p}$ ein Primideal erster Art ist; es lässt sich dann eine Einheit ε^* in $k(\zeta)$ bestimmen, für welche $\left\{\frac{\varepsilon^*\pi^*}{\mathfrak{p}}\right\}=1$ wird und es besteht das Charakterensystem von $\mathfrak{P}^*$ aus dem einen Charakter $\left\{\frac{\varepsilon^*\pi^*,\ \varepsilon\pi}{\mathfrak{l}}\right\}$. Wir entnehmen mithin aus dem Hülfssatz 35 $g\leqq 1$ für den Körper $k(\sqrt[l]{\varepsilon\pi},\zeta)$, d. h. in diesem Körper gehört jede Idealklasse dem Hauptgeschlecht an, und der zuletzt genannte Charakter besitzt daher den Wert 1. Wir haben nun $\left\{\frac{\varepsilon\pi}{\mathfrak{p}^*}\right\}=1$, d. h. wegen der Formel auf S. 366

$$(142.)\qquad \left\{\frac{\mathfrak{p}}{\mathfrak{p}^*}\right\}=\left\{\frac{\varepsilon}{\mathfrak{p}^*}\right\}^{-1};$$

ferner $\left\{\frac{\varepsilon^*\pi^*}{\mathfrak{p}}\right\}=1$, d. h.

$$(143.)\qquad \left\{\frac{\mathfrak{p}^*}{\mathfrak{p}}\right\}=\left\{\frac{\varepsilon^*}{\mathfrak{p}}\right\}^{-1},$$

und endlich $\left\{\frac{\varepsilon^*\pi^*,\ \varepsilon\pi}{\mathfrak{l}}\right\}=1$ oder mit Benutzung von (83.) (S. 413)

$$\left\{\frac{\varepsilon^*,\ \varepsilon}{\mathfrak{l}}\right\}\left\{\frac{\varepsilon^*,\ \pi}{\mathfrak{l}}\right\}\left\{\frac{\pi^*,\ \varepsilon}{\mathfrak{l}}\right\}\left\{\frac{\pi^*,\ \pi}{\mathfrak{l}}\right\}=1.$$

Da nach Hülfssatz 36 $\left\{\frac{\varepsilon^*, \varepsilon}{\mathfrak{l}}\right\} = 1$ und nach Hülfssatz 30 $\left\{\frac{\pi^*, \pi}{\mathfrak{l}}\right\} = 1$ ist, so geht letztere Formel in

$$(144.) \qquad \left\{\frac{\pi,\ \varepsilon^*}{\mathfrak{l}}\right\} = \left\{\frac{\pi^*,\ \varepsilon}{\mathfrak{l}}\right\}$$

über. Da wegen der von uns gemachten Voraussetzung

$$\left\{\frac{\pi, \varepsilon^*}{\mathfrak{l}}\right\} = \left\{\frac{\varepsilon^*}{\mathfrak{p}}\right\} \quad \text{und} \quad \left\{\frac{\pi^*, \varepsilon}{\mathfrak{l}}\right\} = \left\{\frac{\varepsilon}{\mathfrak{p}^*}\right\}$$

ist, so folgt aus (144.) $\left\{\frac{\varepsilon^*}{\mathfrak{p}}\right\} = \left\{\frac{\varepsilon}{\mathfrak{p}^*}\right\}$, und diese Gleichung liefert mit Benutzung der Formeln (142.), (143.) die im Hülfssatz 39 behauptete Gleichung.

Will man wiederum den Satz 151 für $\mathfrak{w} = \mathfrak{l}$ nur in dem Falle eines Körpers $k(\sqrt[l]{\mu}, \zeta)$ anwenden, für den $\mu \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ ausfällt, so wähle man im obigen Beweise die Einheit ε derart, dass man ausser $\left\{\frac{\varepsilon\pi}{\mathfrak{p}^*}\right\} = 1$ noch bei einem geeigneten, zu l primen Exponenten a $(\varepsilon\pi)^a \equiv 1 + \lambda$ nach $\mathfrak{l}^2$ hat. Eine Bestimmung der Einheit ε in dieser Weise ist, wie man leicht sieht, sicher stets dann möglich, wenn $\left\{\frac{\zeta}{\mathfrak{p}^*}\right\} = 1$ ist. Ist aber $\left\{\frac{\zeta}{\mathfrak{p}^*}\right\} \neq 1$ und zugleich $\left\{\frac{\pi}{\mathfrak{p}^*}\right\} \neq 1$, so kann jene Bedingung ebenfalls erfüllt werden, indem man für ε eine geeignete Potenz von ζ nimmt. Ob die fragliche Bedingung sich erfüllen lässt, bleibt also nur dann zweifelhaft, wenn gleichzeitig $\left\{\frac{\zeta}{\mathfrak{p}^*}\right\} \neq 1$ und $\left\{\frac{\pi}{\mathfrak{p}^*}\right\} = 1$ ausfällt. In diesem Falle vertauschen wir bei dem obigen Beweise die Rollen von $\mathfrak{p}$, π einerseits und $\mathfrak{p}^*$, π^* andererseits; dann bleibt offenbar nur noch der Fall unerledigt, dass zugleich $\left\{\frac{\zeta}{\mathfrak{p}^*}\right\} \neq 1$, $\left\{\frac{\zeta}{\mathfrak{p}}\right\} \neq 1$ und $\left\{\frac{\pi}{\mathfrak{p}^*}\right\} = 1$, $\left\{\frac{\pi^*}{\mathfrak{p}}\right\} = 1$ ausfällt. In diesem Falle erkennt man aber aus den letzten zwei Beziehungen die Behauptung des Hülfssatzes 39 ohne Weiteres als richtig.

Hülfssatz 40. Wenn $\mathfrak{p}$ ein Primideal erster Art in $k(\zeta)$ ist und π eine Primärzahl von $\mathfrak{p}$ bedeutet, und wenn für jede beliebige Einheit ξ in $k(\zeta)$ die Gleichung

$$\left\{\frac{\xi}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \xi}{\mathfrak{l}}\right\}$$

besteht, wenn ferner $\mathfrak{p}^*$ ein solches von $\mathfrak{p}$ verschiedenes Primideal erster Art ist, dass

$$\left\{\frac{\mathfrak{p}}{\mathfrak{p}^*}\right\} = \left\{\frac{\mathfrak{p}^*}{\mathfrak{p}}\right\} \neq 1$$

ausfällt, so giebt es stets eine Einheit ε in $k(\zeta)$ von der Art, dass

$$\left\{\frac{\varepsilon}{\mathfrak{p}^*}\right\} = \left\{\frac{\pi^*,\ \varepsilon}{\mathfrak{l}}\right\} \neq 1$$

wird, wobei π^* eine Primärzahl von $\mathfrak{p}^*$ bezeichnet.

Beweis. Wir erfahren zuvörderst genau wie beim Beweise des vorigen Hülfssatzes und gelangen so unter Einführung gewisser Einheiten ε und ε^* wieder zu den drei Formeln (142.), (143.), (144.). Nun ist wegen der Voraussetzung des Hülfssatzes 40 $\left\{\frac{\varepsilon^*}{\mathfrak{p}}\right\} = \left\{\frac{\pi,\ \varepsilon^*}{\mathfrak{l}}\right\}$; hieraus und wegen $\left\{\frac{\mathfrak{p}}{\mathfrak{p}^*}\right\} = \left\{\frac{\mathfrak{p}^*}{\mathfrak{p}}\right\} \neq 1$ folgt in Verbindung mit den drei genannten Formeln die Richtigkeit des Hülfssatzes 40.

Soll Satz 151 nur für den Fall $\mu \equiv 1+\lambda$ nach $\mathfrak{l}^2$ zur Anwendung gelangen, so hat man im vorstehenden Beweise nur nötig, die Einheit ε so zu bestimmen, dass ausser der Gleichung $\left\{\frac{\varepsilon\pi}{\mathfrak{p}^*}\right\} = 1$ noch die Congruenz $(\varepsilon\pi)^a \equiv 1+\lambda$ nach $\mathfrak{l}^2$ bei einem zu l primen Exponenten a erfüllt wird; es ist eine solche Bestimmung von ε hier stets möglich.

§ 157.

Ein besonderer Fall des Reciprocitätsgesetzes für zwei Primideale.

Satz 162. Wenn $\mathfrak{p}$ und $\mathfrak{q}$ irgend zwei beliebige Primideale eines regulären Kreiskörpers sind, für welche $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = 1$ gilt, so ist stets auch $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} = 1$.

Beweis. Es seien π, $\varkappa$ Primärzahlen bez. von $\mathfrak{p}$, $\mathfrak{q}$. Wir betrachten den Kummer'schen Körper $k(\sqrt[l]{\pi}, \zeta)$ und unterscheiden zwei Fälle, je nachdem $\mathfrak{p}$ ein Primideal erster oder zweiter Art ist.

Im ersten Falle erhält die Relativdiscriminante von $k(\sqrt[l]{\pi}, \zeta)$ die zwei Primideale $\mathfrak{l}$ und $\mathfrak{p}$, und es giebt nach Hülfssatz 37 eine Einheit ε in $k(\zeta)$, für welche der Charakter $\left\{\frac{\varepsilon,\ \pi}{\mathfrak{l}}\right\} \neq 1$ ausfällt. Das Charakterensystem eines Ideals in $k(\sqrt[l]{\pi}, \zeta)$ besteht daher nur aus einem Charakter,

d. h. es ist $r=1$ und nach Hülfssatz 35 auch $g=1$. Wegen $\left\{\frac{\pi}{\mathfrak{q}}\right\}=1$ ist $\mathfrak{q}$ in $k(\sqrt[l]{\pi}, \zeta)$ weiter zerlegbar; es sei $\mathfrak{Q}$ ein Primfactor von $\mathfrak{q}$ in diesem Körper. Da π, $\varkappa$ primär sind, so fällt nach Hülfssatz 30 (S. 441) $\left\{\frac{\varkappa, \pi}{\mathfrak{l}}\right\}=1$ aus, und da $\mathfrak{Q}$ zum Hauptgeschlecht gehört, so ist auch $\left\{\frac{\varkappa, \pi}{\mathfrak{p}}\right\}=\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}=1$, wie es der Satz 162 behauptet.

Wenn $\mathfrak{p}$ ein Primideal zweiter Art ist, so gilt nach Hülfssatz 37 für jede Einheit ξ in $k(\zeta)$ die Gleichung $\left\{\frac{\xi, \pi}{\mathfrak{l}}\right\}=1$, und folglich enthält, wie im Beweise des Hülfssatzes 37 gezeigt worden ist, die Relativdiscriminante von $k(\sqrt[l]{\pi}, \zeta)$ nur das eine Primideal $\mathfrak{p}$. Es ist daher wiederum $r=1$ und $g=1$. Wegen $\left\{\frac{\pi}{\mathfrak{q}}\right\}=1$ ist $\mathfrak{q}$ in $k(\sqrt[l]{\pi}, \zeta)$ weiter zerlegbar. Es sei $\mathfrak{Q}$ ein Primfactor von $\mathfrak{q}$ in diesem Körper. Da $\mathfrak{Q}$ zum Hauptgeschlecht gehört, und mit Rücksicht auf $\left\{\frac{\xi, \pi}{\mathfrak{l}}\right\}=1$ ist $\left\{\frac{\varkappa, \pi}{\mathfrak{p}}\right\}=\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}=1$, und damit ist der Satz 162 vollständig bewiesen.

Soll wiederum Satz 151 und dementsprechend auch Hülfssatz 35 für $\mathfrak{w}=\mathfrak{l}$ nur in dem Fall eines Körpers $k(\sqrt[l]{\mu}, \zeta)$, für den $\mu\equiv 1+\lambda$ nach $\mathfrak{l}^2$ ist, angewandt werden, so ist zum Beweise des Satzes 162 im ersten der beiden vorhin unterschiedenen Fälle der folgende Zusatz erforderlich.

Wenn $\mathfrak{p}$ ein beliebiges Primideal und π eine Primärzahl von $\mathfrak{p}$ ist, so erkennen wir aus der Definition des Symbols $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ auf S. 413 und S. 414 und mit Rücksicht auf Hülfssatz 24 (S. 414) die Richtigkeit der Gleichung

$$(145.)\qquad \left\{\frac{\pi, \zeta}{\mathfrak{l}}\right\}=\zeta^{\frac{n(\mathfrak{p})-1}{l}}=\left\{\frac{\zeta}{\mathfrak{p}}\right\}.$$

Ist nun das Primideal $\mathfrak{q}$ von der Beschaffenheit, dass $\left\{\frac{\zeta}{\mathfrak{q}}\right\}=1$ ausfällt, so bestimmen wir eine $l$te Einheitswurzel ζ^* derart, dass $\zeta^*\pi^{l-1}\equiv 1+\lambda$ nach $\mathfrak{l}^2$ ausfällt, und fassen statt des Kummer'schen Körpers $k(\sqrt[l]{\pi}, \zeta)$ den Körper $k(\sqrt[l]{\zeta^*\pi^{l-1}}, \zeta)$ ins Auge. Wir wenden dann die oben dar-

gelegte Schlussweise an. Da

$$\left\{\frac{\varkappa,\ \zeta^*\pi^{l-1}}{\mathfrak{l}}\right\} = \left\{\frac{\varkappa,\ \zeta^*}{\mathfrak{l}}\right\}\left\{\frac{\varkappa,\ \pi}{\mathfrak{l}}\right\}^{l-1}$$

wird und, wie oben, $\left\{\frac{\varkappa,\pi}{\mathfrak{l}}\right\}=1$ ist, andererseits mit Rücksicht auf die in (145.) angegebene Thatsache $\left\{\frac{\varkappa,\zeta}{\mathfrak{l}}\right\}=\left\{\frac{\zeta}{\mathfrak{p}}\right\}=1$ ausfällt, so folgt $\left\{\frac{\varkappa,\zeta^*\pi^{l-1}}{\mathfrak{l}}\right\}=1$, und deshalb schliessen wir $\left\{\frac{\varkappa,\zeta^*\pi^{l-1}}{\mathfrak{p}}\right\}=1$, d. h. $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}=1$.

Es sei andererseits $\left\{\frac{\zeta}{\mathfrak{q}}\right\}\neq 1$. Da $\mathfrak{p}$ ein Primideal erster Art ist, so giebt es sicher eine Einheit ε_1, für welche $\left\{\frac{\varepsilon_1}{\mathfrak{p}}\right\}\neq 1$ ist, und ferner nach Hülfssatz 37 (S. 472) sicher eine Einheit ε_2, für welche $\left\{\frac{\varepsilon_2,\pi}{\mathfrak{l}}\right\}\neq 1$ ausfällt. Auch können wir diese Einheiten ε_1, ε_2 überdies beide so wählen, dass sie $\equiv 1+\lambda$ nach $\mathfrak{l}^2$ sind. Wir entnehmen hieraus weiter die Existenz einer Einheit ε, für welche $\left\{\frac{\varepsilon}{\mathfrak{p}}\right\}\neq 1$ sowie $\left\{\frac{\varepsilon,\pi}{\mathfrak{l}}\right\}\neq 1$ ausfällt und überdies die Congruenzeigenschaft $\varepsilon\equiv 1+\lambda$ nach $\mathfrak{l}^2$ erfüllt ist. In der That, wenn diese Bedingungen weder für $\varepsilon=\varepsilon_1$ noch für $\varepsilon=\varepsilon_2$ zutreffen, so ist gleichzeitig $\left\{\frac{\varepsilon_1,\pi}{\mathfrak{l}}\right\}=1$ und $\left\{\frac{\varepsilon_2}{\mathfrak{p}}\right\}=1$, und dann würde $\varepsilon=(\varepsilon_1\varepsilon_2)^{\frac{l+1}{2}}$ eine Einheit von der verlangten Beschaffenheit sein. Wir bestimmen nun eine solche Potenz $\eta=\varepsilon^a$ der Einheit ε, dass $\left\{\frac{\eta\varkappa}{\mathfrak{p}}\right\}=1$ wird. Wäre nun $\left\{\frac{\varkappa}{\mathfrak{p}}\right\}\neq 1$, so fiele der Exponent a gewiss zu l prim aus, und folglich wäre $\left\{\frac{\eta,\pi}{\mathfrak{l}}\right\}\neq 1$. Es ist ausserdem, da $\varkappa$ eine primäre Zahl darstellt, ersichtlich, dass eine gewisse Potenz von $\eta\varkappa$ mit einem zu l primen Exponenten der Zahl $1+\lambda$ nach $\mathfrak{l}^2$ congruent wird. Aus (145.) und Hülfssatz 36 (S. 471) folgt noch $\left\{\frac{\zeta,\eta\varkappa}{\mathfrak{l}}\right\}\neq 1$. Der Kummer'sche Körper $k(\sqrt[l]{\eta\varkappa},\zeta)$ besitzt desshalb nur ein Geschlecht. Wegen $\left\{\frac{\eta\varkappa}{\mathfrak{p}}\right\}=1$ ist $\mathfrak{p}$ in diesem Körper weiter zerlegbar; ist $\mathfrak{P}$ ein

in $\mathfrak{p}$ aufgehender Primfactor dieses Körpers, so findet man den Charakter von $\mathfrak{P}$ gleich dem Symbol

$$\left\{\frac{\zeta^*\pi,\ \eta\varkappa}{\mathfrak{q}}\right\} = \left\{\frac{\zeta^*\pi}{\mathfrak{q}}\right\},$$

wenn ζ^* eine solche $l$te Einheitswurzel bedeutet, dass $\left\{\frac{\zeta^*\pi,\ \eta\varkappa}{\mathfrak{l}}\right\} = 1$ ausfällt. Wegen der letzten Gleichung, und da $\left\{\frac{\zeta,\ \eta}{\mathfrak{l}}\right\} = 1$ ist, folgt $\left\{\frac{\zeta^*,\ \varkappa}{\mathfrak{l}}\right\}\left\{\frac{\pi,\ \eta}{\mathfrak{l}}\right\} = 1$, und wegen $\left\{\frac{\pi,\ \eta}{\mathfrak{l}}\right\} \neq 1$ ist also auch $\left\{\frac{\zeta^*,\ \varkappa}{\mathfrak{l}}\right\} \neq 1$, d. i. mit Rücksicht auf (145.) $\left\{\frac{\zeta^*}{\mathfrak{q}}\right\} \neq 1$; somit ist $\zeta^* \neq 1$. Da aber jener eine Charakter des Primideals $\mathfrak{P}$ gleich 1 sein muss, so folgt wegen $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = 1$ notwendig auch $\left\{\frac{\zeta^*}{\mathfrak{q}}\right\} = 1$, und dies stünde im Widerspruch mit der eben gezogenen Folgerung.

§ 158.

Das Vorhandensein gewisser Hülfsprimideale, für welche das Reciprocitätsgesetz gilt.

Auf Grund der Sätze 152, 140 und 162 erkennen wir leicht die Existenz gewisser Primideale, die in § 159 und § 160 zur Verwendung kommen werden. Es gelten folgende Thatsachen:

Hülfssatz 41. Wenn $\mathfrak{p}$ ein beliebiges Primideal des regulären Kreiskörpers $k(\zeta)$ bedeutet, so giebt es stets ein Primideal $\mathfrak{r}$ in $k(\zeta)$, welches den Bedingungen

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\} \neq 1, \quad \left\{\frac{\mathfrak{p}}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{p}}\right\} \neq 1$$

genügt.

Beweis. Es sei h die Klassenanzahl von $k(\zeta)$ und, wie in § 149 und § 154, h^* eine positive ganze rationale Zahl, so dass $hh^* \equiv 1$ nach l wird. Es sei p die rationale, durch $\mathfrak{p}$ teilbare Primzahl und $\pi = \mathfrak{p}^{hh^*}$ eine Primärzahl von $\mathfrak{p}$; ferner seien $\mathfrak{p}', \mathfrak{p}'', \ldots$ die unter einander und von $\mathfrak{p}$ verschiedenen, zu $\mathfrak{p}$ conjugirten Primideale in $k(\zeta)$ und $\pi' = \mathfrak{p}'^{hh^*}$, $\pi'' = \mathfrak{p}''^{hh^*}$ die betreffenden zu π conjugirten Zahlen in $k(\zeta)$; sie sind Primärzahlen bez. von $\mathfrak{p}', \mathfrak{p}'', \ldots$. Wir haben dann $p = \mathfrak{p}\mathfrak{p}'\mathfrak{p}'' \ldots$; da ferner $\dfrac{p^{hh^*}}{\pi\pi'\pi'' \ldots}$ eine Einheit in $k(\zeta)$ sein muss und überdies primär ausfällt, so stellt nach Satz 156 (s. auch S. 441) dieser Quotient die

$l$te Potenz einer Einheit ε in $k(\zeta)$ dar, es ist also

$$p^{hh^*} = \varepsilon^l \pi\pi'\pi'' \ldots.$$

Nunmehr wenden wir den Satz 152 (S. 426) an, indem wir dort

$$\alpha_1 = \zeta, \quad \alpha_2 = \pi, \quad \alpha_3 = \pi', \quad \alpha_4 = \pi'', \quad \alpha_5 = \pi''', \quad \ldots,$$
$$\gamma_1 = \zeta, \quad \gamma_2 = \zeta, \quad \gamma_3 = 1, \quad \gamma_4 = 1, \quad \gamma_5 = 1, \quad \ldots$$

nehmen. Da ζ nicht die $l$te Potenz einer Einheit in $k(\zeta)$ ist und $\pi, \pi', \pi'', \ldots$ Potenzen von Primidealen sind, deren Exponenten zu l prim ausfallen, so sind die Voraussetzungen des Satzes 152 erfüllt, und es giebt daher nach diesem Satze in $k(\zeta)$ ein Primideal $\mathfrak{r}$, für welches bei irgend einem geeigneten, zu l primen Exponenten m

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\}^m = \zeta, \quad \left\{\frac{\pi}{\mathfrak{r}}\right\}^m = \zeta, \quad \left\{\frac{\pi'}{\mathfrak{r}}\right\}^m = 1, \quad \left\{\frac{\pi''}{\mathfrak{r}}\right\}^m = 1, \quad \ldots,$$

d. h.

$$(146.) \quad \left\{\frac{\zeta}{\mathfrak{r}}\right\} = \zeta^*, \left\{\frac{\pi}{\mathfrak{r}}\right\} = \zeta^*, \left\{\frac{\pi'}{\mathfrak{r}}\right\} = 1, \left\{\frac{\pi''}{\mathfrak{r}}\right\} = 1, \ldots$$

wird, wo ζ^* eine von 1 verschiedene $l$te Einheitswurzel darstellt. Aus (146.) erhalten wir $\left\{\frac{p^{hh^*}}{\mathfrak{r}}\right\} = \left\{\frac{\varepsilon^{-l} p^{hh^*}}{\mathfrak{r}}\right\} = \left\{\frac{\pi\pi'\pi''\ldots}{\mathfrak{r}}\right\} = \zeta^*$, und folglich wird wegen Satz 140 (S. 369) auch $\left\{\frac{\varrho}{p^{hh^*}}\right\} = \zeta^*$, wo ϱ eine Primärzahl von $\mathfrak{r}$ bedeuten soll. Da nun wegen (146.) nach Satz 162 (S. 479) $\left\{\frac{\varrho}{\pi'}\right\} = 1, \left\{\frac{\varrho}{\pi''}\right\} = 1, \ldots$ sein muss und

$$\left\{\frac{\varrho}{p^{hh^*}}\right\} = \left\{\frac{\varrho}{\pi}\right\}\left\{\frac{\varrho}{\pi'}\right\}\left\{\frac{\varrho}{\pi''}\right\}\ldots$$

ist, so erhalten wir $\left\{\frac{\varrho}{\pi}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{p}}\right\} = \zeta^*$; damit ist gezeigt, dass das Primideal $\mathfrak{r}$ alle Bedingungen des Hülfssatzes 41 erfüllt.

Hülfssatz 42. Wenn $\mathfrak{p}$ ein beliebiges Primideal des regulären Kreiskörpers $k(\zeta)$ und π eine Primärzahl von $\mathfrak{p}$ bedeutet, wenn ferner ε eine beliebige Einheit in $k(\zeta)$, nur nicht die $l$te Potenz einer Einheit in $k(\zeta)$ ist, so giebt es ein Primideal $\mathfrak{r}$ in $k(\zeta)$, das den Bedingungen

$$\left\{\frac{\varepsilon\pi}{\mathfrak{r}}\right\} = 1, \quad \left\{\frac{\mathfrak{p}}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{p}}\right\} \neq 1$$

genügt.

Beweis. Es mögen π, π', π'', ... für $\mathfrak{p}$ die Bedeutung wie im vorigen Hülfssatz 41 haben; wir nehmen in Satz 152 (S. 426)

$$\alpha_1 = \varepsilon\pi, \quad \alpha_2 = \pi, \quad \alpha_3 = \pi', \quad \alpha_4 = \pi'', \quad \alpha_5 = \pi''', \quad \ldots$$

$$\gamma_1 = 1, \quad \gamma_2 = \zeta, \quad \gamma_3 = 1, \quad \gamma_4 = 1, \quad \gamma_5 = 1, \quad \ldots;$$

die Zahlen α_1, α_2, α_3, α_4, α_5, ... genügen wiederum, wie man leicht einsieht, der Voraussetzung des Satzes 152; es führt die entsprechende Schlussweise wie in Hülfssatz 41 zu einem Primideal $\mathfrak{r}$ von der hier verlangten Beschaffenheit.

§ 159.

Beweis des ersten Ergänzungssatzes zum Reciprocitätsgesetz.

Um den ersten Ergänzungssatz für ein Primideal $\mathfrak{p}$ der ersten Art zu beweisen, wenden wir den Hülfssatz 41 an; diesem zufolge lässt sich ein Primideal $\mathfrak{r}$ bestimmen, für welches

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\} \neq 1 \quad \text{und} \quad \left\{\frac{\mathfrak{r}}{\mathfrak{p}}\right\} = \left\{\frac{\mathfrak{p}}{\mathfrak{r}}\right\} \neq 1$$

wird, und das also gewiss ein Primideal erster Art ist. Nach Gleichung (145.) haben wir für das Primideal $\mathfrak{r}$ die Gleichung

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\} = \zeta^{\frac{n(\mathfrak{r})-1}{l}} = \left\{\frac{\varrho,\, \zeta}{\mathfrak{l}}\right\},$$

wo ϱ eine Primärzahl von $\mathfrak{r}$ bedeuten soll. Da $\left\{\frac{\zeta}{\mathfrak{r}}\right\} \neq 1$ ausfällt, so besteht nach Hülfssatz 38 (S. 475) auch für jede andere Einheit ξ in $k(\zeta)$ die Gleichung

$$\left\{\frac{\xi}{\mathfrak{r}}\right\} = \left\{\frac{\varrho,\, \xi}{\mathfrak{l}}\right\},$$

und demnach treffen die sämtlichen Bedingungen des Hülfssatzes 40 (S. 478) zu, wenn wir an Stelle der dort mit $\mathfrak{p}$ bez. $\mathfrak{p}^*$ bezeichneten Primideale die beiden Primideale $\mathfrak{r}$ bez. $\mathfrak{p}$ nehmen. Nach jenem Hülfssatze giebt es somit eine Einheit ε in $k(\zeta)$ derart, dass $\left\{\frac{\varepsilon}{\mathfrak{p}}\right\} = \left\{\frac{\pi,\, \varepsilon}{\mathfrak{l}}\right\} \neq 1$ wird, wobei π eine Primärzahl von $\mathfrak{p}$ bedeuten soll. Infolge dieser Thatsache ist nach Hülfssatz 38 (S. 475) auch für jede andere Einheit ξ in $k(\zeta)$ die Gleichung $\left\{\frac{\xi}{\mathfrak{p}}\right\} = \left\{\frac{\pi,\, \xi}{\mathfrak{l}}\right\}$ erfüllt, wie es der erste Ergänzungssatz behauptet.

Des Weiteren bedeute $\mathfrak{q}$ ein Primideal zweiter Art in $k(\zeta)$. Dann ist nach der Definition eines solchen Primideals für jede Einheit ξ in $k(\zeta)$ stets $\left\{\frac{\xi}{\mathfrak{q}}\right\}=1$, und wenn $\varkappa$ eine Primärzahl von $\mathfrak{q}$ bezeichnet, so ist nach Hülfssatz 37 (S. 472) stets auch $\left\{\frac{\varkappa, \xi}{\mathfrak{l}}\right\}=1$. Es gilt daher in der That wiederum der erste Ergänzungssatz $\left\{\frac{\xi}{\mathfrak{q}}\right\}=\left\{\frac{\varkappa, \xi}{\mathfrak{l}}\right\}$.

§ 160.

Beweis des Reciprocitätsgesetzes zwischen zwei beliebigen Primidealen.

Nachdem der erste Ergänzungssatz in § 159 bewiesen worden ist, folgt aus Hülfssatz 39 (S. 476) sofort die Richtigkeit des Reciprocitätsgesetzes für zwei beliebige Primideale erster Art.

Es sei zweitens ein Primideal $\mathfrak{p}$ erster Art und ein Primideal $\mathfrak{q}$ zweiter Art vorgelegt; π und $\varkappa$ seien Primärzahlen von $\mathfrak{p}$ und $\mathfrak{q}$. Im Falle, dass $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}=1$ ausfällt, folgt aus Satz 162 (S. 479) $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}=1$ und mithin die Richtigkeit des Reciprocitätsgesetzes für $\mathfrak{p}$ und $\mathfrak{q}$. Wir nehmen jetzt an, es sei $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}=\left\{\frac{\varkappa}{\mathfrak{p}}\right\}\neq 1$. Da $\mathfrak{p}$ von der ersten Art ist, so giebt es eine Einheit ε, so dass $\left\{\frac{\varepsilon\varkappa}{\mathfrak{p}}\right\}=1$ ausfällt, und es kann hierbei stets, wie aus einer Betrachtung am Schlusse des Beweises von Hülfssatz 39 (S. 476) hervorgeht, die Einheit ε zugleich so bestimmt werden, dass eine gewisse Potenz von $\varepsilon\varkappa$ mit einem zu l primen Exponenten $\equiv 1+\lambda$ nach $\mathfrak{l}^2$ wird. Wir betrachten den Kummer'schen Körper $k(\sqrt[l]{\varepsilon\varkappa}, \zeta)$. Nach Satz 148 (S. 393) enthält die Relativdiscriminante dieses Körpers in Bezug auf $k(\zeta)$ die zwei Primfactoren $\mathfrak{l}$ und $\mathfrak{q}$. Da $\mathfrak{q}$ ein Primideal zweiter Art ist, so gelten wegen der Hülfssätze 36 und 37 für jede Einheit ξ in $k(\zeta)$ die Gleichungen

$$\left\{\frac{\xi, \varepsilon\varkappa}{\mathfrak{l}}\right\}=\left\{\frac{\xi, \varepsilon}{\mathfrak{l}}\right\}\left\{\frac{\xi, \varkappa}{\mathfrak{l}}\right\}=1, \quad \left\{\frac{\xi}{\mathfrak{q}}\right\}=1,$$

und demgemäss ist die Anzahl r der Charaktere, welche das Geschlecht eines Ideals in $k(\sqrt[l]{\varepsilon\varkappa}, \zeta)$ bestimmen, gleich 2. Nach Hülfssatz 35 (S. 470) ist dann in $k(\sqrt[l]{\varepsilon\varkappa}, \zeta)$ die Anzahl der Geschlechter $g\leq l$. Wir bestimmen

nun nach Hülfssatz 42 (S. 483) ein Primideal $\mathfrak{r}$ in $k(\zeta)$ von der Beschaffenheit, dass

$$\left\{\frac{\varepsilon\varkappa}{\mathfrak{r}}\right\}=1,\quad \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}=\left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}\neq 1$$

wird. Wegen der ersteren Gleichung ist $\mathfrak{r}$ in $k(\sqrt[l]{\varepsilon\varkappa},\zeta)$ weiter zerlegbar. Es sei $\mathfrak{R}$ ein Primfactor von $\mathfrak{r}$ in diesem Körper und ϱ eine Primärzahl von $\mathfrak{r}$. Dann besteht das Charakterensystem des Ideals $\mathfrak{R}$ in $k(\sqrt[l]{\varepsilon\varkappa},\zeta)$ aus den beiden Charakteren

$$\left\{\frac{\varrho,\,\varepsilon\varkappa}{\mathfrak{l}}\right\},\quad \left\{\frac{\varrho,\,\varepsilon\varkappa}{\mathfrak{q}}\right\}=\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}. \tag{147.}$$

Da der zweite Charakter $\neq 1$ ist, so bestimmen die Ideale $\mathfrak{R},\mathfrak{R}^2,\ldots,\mathfrak{R}^l$ lauter von einander verschiedene Geschlechter, und es giebt, wie die oben gefundene obere Grenze für die Anzahl der Geschlechter zeigt, ausser diesen keine weiteren Geschlechter. Mit Benutzung des in § 159 bewiesenen ersten Ergänzungssatzes ergiebt sich

$$\left\{\frac{\varrho,\,\varepsilon\varkappa}{\mathfrak{l}}\right\}\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}=\left\{\frac{\varrho,\,\varepsilon}{\mathfrak{l}}\right\}\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}=\left\{\frac{\varepsilon}{\mathfrak{r}}\right\}\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}$$

$$=\left\{\frac{\varepsilon}{\mathfrak{r}}\right\}\left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}=\left\{\frac{\varepsilon\varkappa}{\mathfrak{r}}\right\}=1,$$

d. h. das Product der beiden Charaktere (147.) ist gleich 1. Da jedes beliebige Ideal in $k(\sqrt[l]{\varepsilon\varkappa},\zeta)$ notwendig einem jener l Geschlechter angehören muss, so folgt hieraus, dass für jedes Ideal in $k(\sqrt[l]{\varepsilon\varkappa},\zeta)$ das Product seiner beiden Charaktere stets gleich 1 ist. Wegen $\left\{\frac{\varepsilon\varkappa}{\mathfrak{p}}\right\}=1$ ist $\mathfrak{p}$ in $k(\sqrt[l]{\varepsilon\varkappa},\zeta)$ weiter zerlegbar; bezeichnet $\mathfrak{P}$ einen Primfactor von $\mathfrak{p}$ in diesem Körper, so sind die beiden Charaktere für $\mathfrak{P}$ durch die Symbole

$$\left\{\frac{\pi,\,\varepsilon\varkappa}{\mathfrak{l}}\right\},\quad \left\{\frac{\pi,\,\varepsilon\varkappa}{\mathfrak{q}}\right\}=\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}$$

gegeben, und es folgt somit unter Benutzung des in § 159 bewiesenen Ergänzungssatzes notwendig

$$\left\{\frac{\pi,\,\varepsilon\varkappa}{\mathfrak{l}}\right\}\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}=\left\{\frac{\pi,\,\varepsilon}{\mathfrak{l}}\right\}\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}=\left\{\frac{\varepsilon}{\mathfrak{p}}\right\}\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}=1$$

oder

$$\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}=\left\{\frac{\varepsilon}{\mathfrak{p}}\right\}^{-1}=\left\{\frac{\varkappa}{\mathfrak{p}}\right\}=\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\},$$

d. h. es gilt das Reciprocitätsgesetz für die beiden Primideale $\mathfrak{p}$ und $\mathfrak{q}$.

Es seien drittens zwei Primideale $\mathfrak{q}$ und $\mathfrak{q}^*$ der zweiten Art vorgelegt; $\varkappa$, $\varkappa^*$ seien Primärzahlen von $\mathfrak{q}$ bez. $\mathfrak{q}^*$. Wir betrachten den Kummer'schen Körper $k(\sqrt[l]{\varkappa\varkappa^*}, \zeta)$. Die Zahlen $\varkappa$ und $\varkappa^*$ sind, wie sich im Beweise des Hülfssatzes 37 herausgestellt hat, $l$ten Potenzen von gewissen ganzen Zahlen in $k(\zeta)$ nach $\mathfrak{l}^l$ congruent; das Gleiche gilt daher von $\varkappa\varkappa^*$, und folglich ist nach Satz 148 (S. 393) die Relativdiscriminante des Körpers $k(\sqrt[l]{\varkappa\varkappa^*}, \zeta)$ nicht durch $\mathfrak{l}$ teilbar. Diese Relativdiscriminante enthält somit nur die beiden Primfactoren $\mathfrak{q}$ und $\mathfrak{q}^*$. Nun ist für jede Einheit ξ in $k(\zeta)$

$$\left\{\frac{\xi,\ \varkappa\varkappa^*}{\mathfrak{q}}\right\}=\left\{\frac{\xi}{\mathfrak{q}}\right\}=1,\quad \left\{\frac{\xi,\ \varkappa\varkappa^*}{\mathfrak{q}^*}\right\}=\left\{\frac{\xi}{\mathfrak{q}^*}\right\}=1,$$

und dementsprechend ist die Anzahl r der Charaktere, welche das Geschlecht eines Ideals in $k(\sqrt[l]{\varkappa\varkappa^*}, \zeta)$ bestimmen, $=2$. Nach Hülfssatz 35 (S. 470) ist dann in $k(\sqrt[l]{\varkappa\varkappa^*}, \zeta)$ die Anzahl der Geschlechter $g \leqq l$. Ferner lässt sich nach Satz 152 (S. 426) jedenfalls ein Primideal $\mathfrak{r}$ in $k(\zeta)$ bestimmen derart, dass

$$\left\{\frac{\varkappa\varkappa^*}{\mathfrak{r}}\right\}=1,\quad \left\{\frac{\zeta}{\mathfrak{r}}\right\}\neq 1,\quad \left\{\frac{\varkappa}{\mathfrak{r}}\right\}\neq 1$$

ausfällt. Wegen der ersten Gleichung ist $\mathfrak{r}$ in $k(\sqrt[l]{\varkappa\varkappa^*}, \zeta)$ weiter zerlegbar; es sei $\mathfrak{R}$ ein Primfactor von $\mathfrak{r}$ in diesem Körper und ϱ eine Primärzahl von $\mathfrak{r}$. Dann besteht das Charakterensystem des Ideals $\mathfrak{R}$ in $k(\sqrt[l]{\varkappa\varkappa^*}, \zeta)$ aus den beiden Charakteren

$$(148.)\qquad \begin{cases} \left\{\frac{\varrho,\ \varkappa\varkappa^*}{\mathfrak{q}}\right\}=\left\{\frac{\varrho}{\mathfrak{q}}\right\}=\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}, \\ \left\{\frac{\varrho,\ \varkappa\varkappa^*}{\mathfrak{q}^*}\right\}=\left\{\frac{\varrho}{\mathfrak{q}^*}\right\}=\left\{\frac{\mathfrak{r}}{\mathfrak{q}^*}\right\}. \end{cases}$$

Da der erste Charakter wegen $\left\{\frac{\varkappa}{\mathfrak{r}}\right\}\neq 1$ dem Satze 162 (S. 479) gemäss

notwendig ebenfalls verschieden von 1 ist, so bestimmen die Ideale $\mathfrak{R}, \mathfrak{R}^2, \ldots, \mathfrak{R}^l$ lauter von einander verschiedene Geschlechter, und es giebt, wie bereits gezeigt worden ist, auch hier nicht mehr als l Geschlechter. Wegen $\left\{\frac{\zeta}{\mathfrak{r}}\right\} \neq 1$ ist $\mathfrak{r}$ ein Primideal erster Art; es gilt daher nach dem Vorigen einerseits für die Primideale $\mathfrak{r}, \mathfrak{q}$, andererseits für die Primideale $\mathfrak{r}, \mathfrak{q}^*$ das Reciprocitätsgesetz, und das Product der beiden Charaktere (148.) wird folglich

$$(149.) \qquad \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}\left\{\frac{\mathfrak{r}}{\mathfrak{q}^*}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}\left\{\frac{\mathfrak{q}^*}{\mathfrak{r}}\right\} = \left\{\frac{\varkappa\varkappa^*}{\mathfrak{r}}\right\} = 1.$$

Da jedes beliebige Ideal in $k(\sqrt[l]{\varkappa\varkappa^*}, \zeta)$ einem jener l Geschlechter angehören muss, so folgt aus (149.), dass für jedes Ideal das Product seiner beiden Charaktere gleich 1 sein muss. Nun ist das Ideal $\mathfrak{q}$ gleich der $l$ten Potenz eines Primideals $\mathfrak{Q}$ in $k(\sqrt[l]{\varkappa\varkappa^*}, \zeta)$. Die beiden Charaktere von $\mathfrak{Q}$ in diesem Körper sind alsdann

$$\left\{\frac{\varkappa,\ \varkappa\varkappa^*}{\mathfrak{q}}\right\} = \left\{\frac{\varkappa^*,\ \varkappa\varkappa^*}{\mathfrak{q}}\right\}^{-1} = \left\{\frac{\varkappa^*}{\mathfrak{q}}\right\}^{-1} = \left\{\frac{\mathfrak{q}^*}{\mathfrak{q}}\right\}^{-1},$$

$$\left\{\frac{\varkappa,\ \varkappa\varkappa^*}{\mathfrak{q}^*}\right\} = \left\{\frac{\varkappa}{\mathfrak{q}^*}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{q}^*}\right\},$$

und da ihr Product gleich 1 sein soll, so erhalten wir

$$\left\{\frac{\mathfrak{q}^*}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{q}^*}\right\}.$$

Hiermit ist das Reciprocitätsgesetz für zwei Primideale der zweiten Art bewiesen, und nunmehr ist der Beweis des Reciprocitätsgesetzes für zwei beliebige Primideale vollständig erbracht.

§ 161.

Beweis des zweiten Ergänzungssatzes zum Reciprocitätsgesetz.

Es sei zunächst $\mathfrak{p}$ ein Primideal erster Art und π eine Primärzahl von $\mathfrak{p}$. Wir bestimmen eine Einheit ε in $k(\zeta)$ derart, dass $\left\{\frac{\varepsilon\lambda}{\mathfrak{p}}\right\} = 1$ wird, und betrachten dann den durch $\sqrt[l]{\varepsilon\lambda}$ und ζ bestimmten Kummer'schen Körper. Wegen $\left\{\frac{\varepsilon\lambda}{\mathfrak{p}}\right\} = 1$ ist $\mathfrak{p}$ in diesem Körper weiter zerlegbar; es

sei $\mathfrak{P}$ ein Primfactor von $\mathfrak{p}$ in diesem Körper. Wir erkennen, dass das Charakterensystem des Ideals $\mathfrak{P}$ aus dem einen Charakter $\left\{\frac{\pi, \varepsilon\lambda}{\mathfrak{l}}\right\}$ besteht, und da somit nach Hülfssatz 35 (S. 470) auch nur ein Geschlecht, nämlich das Hauptgeschlecht, vorhanden ist, so muss dieser Charakter den Wert 1 besitzen. Hieraus, und da nach § 159 $\left\{\frac{\varepsilon}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \varepsilon}{\mathfrak{l}}\right\}$ ist, folgt sofort die Gleichung $\left\{\frac{\lambda}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \lambda}{\mathfrak{l}}\right\}$.

Des Weiteren sei ein Primideal $\mathfrak{q}$ der zweiten Art vorgelegt, und es bezeichne $\varkappa$ eine Primärzahl von $\mathfrak{q}$; dann sind zwei Fälle zu unterscheiden, je nachdem $\left\{\frac{\lambda}{\mathfrak{q}}\right\} = 1$ oder $\neq 1$ ausfällt. Im ersteren Falle lehrt die Betrachtung des Kummer'schen Körpers $k(\sqrt[l]{\lambda}, \zeta)$, dass auch $\left\{\frac{\varkappa, \lambda}{\mathfrak{l}}\right\} = 1$ ist. Im zweiten Falle bestimme man nach Satz 152 (S. 426) ein Primideal $\mathfrak{p}$, für welches $\left\{\frac{\zeta}{\mathfrak{p}}\right\} = \left\{\frac{\varkappa}{\mathfrak{p}}\right\}^{-1} \neq 1$ ausfällt. Dann ist $\mathfrak{p}$ gewiss ein Primideal erster Art, und es folgt nach Satz 162 (S. 479), wenn π eine Primärzahl von $\mathfrak{p}$ bedeutet, $\left\{\frac{\pi}{\mathfrak{q}}\right\} \neq 1$; mithin lässt sich gewiss eine ganze rationale Zahl a so bestimmen, dass $\left\{\frac{\lambda\pi^a}{\mathfrak{q}}\right\} = 1$ ausfällt. Betrachten wir den Körper $k(\sqrt[l]{\lambda\pi^a}, \zeta)$, so besteht für diesen, weil $\left\{\frac{\zeta, \lambda\pi^a}{\mathfrak{p}}\right\} = \left\{\frac{\zeta}{\mathfrak{p}}\right\}^a \neq 1$ ist, das Charakterensystem eines Ideals wiederum nur aus einem Charakter, und dieser ist stets gleich 1. Wenden wir die letztere Thatsache auf einen Primfactor $\mathfrak{Q}$ von $\mathfrak{q}$ in diesem Körper an, so folgt $\left\{\frac{\zeta\varkappa, \lambda\pi^a}{\mathfrak{l}}\right\} = \left\{\frac{\zeta}{\mathfrak{p}}\right\}^{-a}\left\{\frac{\varkappa, \lambda}{\mathfrak{l}}\right\} = 1$, und berücksichtigen wir die Gleichung $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}$, so entsteht $\left\{\frac{\lambda}{\mathfrak{q}}\right\} = \left\{\frac{\varkappa, \lambda}{\mathfrak{l}}\right\}$.

Das Reciprocitätsgesetz für $l$te Potenzreste ist zuerst von *Kummer* bewiesen worden. Der hier dargelegte neue Beweis desselben unterscheidet sich von den *Kummer*'schen Beweisen vor allem darin, dass *Kummer* zunächst den ersten Ergänzungssatz, und zwar unter einem erheblichen Aufwande von Rechnung, durch eine kunstvolle Erweiterung der Formeln der Kreisteilung gewinnt und dann erst auf Grund der errechneten Formeln das Reciprocitätsgesetz zwischen zwei Primidealen ableitet, während die

obige Entwickelung die Beweisgründe für das Reciprocitätsgesetz und seine beide Ergänzungssätze aus gemeinsamer Quelle schöpft.

Von besonderen Reciprocitätsgesetzen, zu deren Behandlung die Formeln der Kreisteilung ausreichen, sind das Reciprocitätsgesetz für biquadratische Reste [*Gauss*[3], *Eisenstein*[8, 9]], das Reciprocitätsgesetz für cubische Reste [*Eisenstein*[5, 7], *Jacobi*[1]], ferner für bicubische Reste [*Gmeiner*[1, 2, 3]] und die auf 5te, 8te, 12te Potenzreste bezüglichen Untersuchungen von *Jacobi* zu nennen [*Jacobi*[4]].

Auch sei endlich noch erwähnt, dass *Eisenstein* ohne Beweis ein Reciprocitätsgesetz für $l$te Potenzreste aufgestellt und dabei auch den Fall in Betracht gezogen hat, dass die Klassenanzahl des Kreiskörpers der $l$ten Einheitswurzeln durch l teilbar ist. [*Eisenstein*[1, 12].]

Capitel XXXIV.

Die Anzahl der vorhandenen Geschlechter im regulären Kummer'schen Körper.

§ 162.

Ein Satz über das Symbol $\left\{\frac{\nu,\mu}{\mathfrak{w}}\right\}$.

Die wichtigste Aufgabe in der Theorie der Geschlechter eines Kummer'schen Körpers betrifft die Ermittelung der Anzahl der wirklich vorhandenen Geschlechter. Wir beweisen hier zunächst einen Satz, welcher dem Hülfssatze 14 (S. 297) aus der Theorie des quadratischen Körpers entspricht.

Satz 163. Wenn ν und μ zwei beliebige ganze Zahlen ($\neq 0$) eines regulären Kreiskörpers $k(\zeta)$ bedeuten, so ist stets

$$\prod_{(\mathfrak{w})}\left\{\frac{\nu,\ \mu}{\mathfrak{w}}\right\} = 1,$$

wenn das Product linker Hand über sämtliche Primideale $\mathfrak{w}$ in $k(\zeta)$ erstreckt wird.

Beweis. Es sei h die Anzahl der Idealklassen in $k(\zeta)$ und h^* eine ganze rationale positive Zahl mit der Congruenzeigenschaft $hh^* \equiv 1$ nach l. Wir setzen $\nu = \mathfrak{l}^a\mathfrak{p}_1\mathfrak{p}_2\cdots$ und $\mu = \mathfrak{l}^b\mathfrak{q}_1\mathfrak{q}_2\cdots$, so dass a

und b ganze rationale Exponenten und $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{q}_1, \mathfrak{q}_2, \ldots$ gewisse von $\mathfrak{l}$ verschiedene Primideale in $k(\zeta)$ sind. Bedeuten ferner $\pi_1, \pi_2, \ldots, \varkappa_1, \varkappa_2, \ldots$ Primärzahlen der Primideale bez. $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{q}_1, \mathfrak{q}_2, \ldots$, und zwar derart, dass

$$\pi_1 = \mathfrak{p}_1^{hh^*}, \quad \pi_2 = \mathfrak{p}_2^{hh^*}, \quad \ldots, \quad \varkappa_1 = \mathfrak{q}_1^{hh^*}, \quad \varkappa_2 = \mathfrak{q}_2^{hh^*}, \quad \ldots$$

gilt, und wird noch $\lambda = 1 - \zeta$ gesetzt, so bestehen zwei Gleichungen von der Gestalt:

$$(150.) \qquad \nu^{hh^*} = \varepsilon \lambda^{ahh^*} \pi_1 \pi_2 \cdots, \quad \mu^{hh^*} = \eta \lambda^{bhh^*} \varkappa_1 \varkappa_2 \cdots,$$

worin ε und η Einheiten in $k(\zeta)$ sind. Wenn $\mathfrak{w}$ ein beliebiges Primideal bedeutet, so ist allgemein

$$(151.) \qquad \left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = \left\{\frac{\nu^{hh^*}, \mu^{hh^*}}{\mathfrak{w}}\right\}.$$

Es seien nun $\mathfrak{p}, \mathfrak{q}$ zwei von einander und von $\mathfrak{l}$ verschiedene Primideale in $k(\zeta)$ und $\pi, \varkappa$ bez. Primärzahlen von $\mathfrak{p}, \mathfrak{q}$; ferner seien ε, η beliebige Einheiten in $k(\zeta)$. Aus Hülfssatz 36 (S. 471) und aus Satz 161 (S. 471) folgen dann leicht die Formeln

$$(152.) \qquad \begin{cases} \left\{\dfrac{\varepsilon, \eta}{\mathfrak{l}}\right\} = 1, \quad \left\{\dfrac{\varepsilon, \lambda}{\mathfrak{l}}\right\} = 1, \\ \left\{\dfrac{\varepsilon, \pi}{\mathfrak{l}}\right\}\left\{\dfrac{\varepsilon, \pi}{\mathfrak{p}}\right\} = 1, \quad \left\{\dfrac{\pi, \varkappa}{\mathfrak{p}}\right\}\left\{\dfrac{\pi, \varkappa}{\mathfrak{q}}\right\} = 1. \end{cases}$$

Ist $\mathfrak{w}$ ein von $\mathfrak{l}$ verschiedenes Primideal, welches nicht in μ aufgeht, so ist nach Satz 148 (S. 393) die Relativdiscriminante des Kummer'schen Körpers $k(\sqrt[l]{\mu}, \zeta)$ zu $\mathfrak{w}$ prim; fällt dann $\mathfrak{w}$ auch zu ν prim aus, so ist nach Satz 150 (S. 402) die Zahl ν Normenrest des Kummer'schen Körpers $k(\sqrt[l]{\mu}, \zeta)$, und daher gilt nach Satz 151 (S. 420) die Gleichung $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = 1$. Mit Rücksicht hierauf gilt wegen (152.) der Satz für den Fall, dass eine jede der Zahlen ν, μ sei es eine Einheit, sei es eine beliebige Potenz von λ, sei es eine Primärzahl eines von $\mathfrak{l}$ verschiedenen Primideals vorstellt; wegen (150.) und (151.) und auf Grund der Regeln (80.) (S. 411) und (83.) (S. 413) gilt sodann der Satz 163 allgemein.

§ 163.

Der Fundamentalsatz über die Geschlechter eines regulären Kummer'schen Körpers.

Wir sind jetzt im Stande, für den regulären Kummer'schen Körper denjenigen Satz aufzustellen und zu beweisen, welcher dem fundamentalen Satz 100 (S. 293) in der Theorie des quadratischen Körpers entspricht. Dieser Satz lautet:

Satz 164. *Es sei r die Anzahl der Charaktere, welche ein Geschlecht im regulären Kummer'schen Körper $K=k(\sqrt[l]{\mu},\zeta)$ bestimmen; ist dann ein System von r beliebigen $l$ten Einheitswurzeln vorgelegt, so ist dieses System dann und nur dann das Charakterensystem eines Geschlechtes in K, wenn das Product der sämtlichen r Einheitswurzeln gleich* 1 *ist. Die Anzahl der in K vorhandenen Geschlechter ist daher gleich l^{r-1}.*

Beweis. Es sei h die Klassenanzahl des regulären Kreiskörpers $k(\zeta)$ und h^* eine ganze rationale positive Zahl mit der Congruenzeigenschaft $hh^*\equiv 1$ nach l; ferner seien $\mathfrak{l}_1,\ldots,\mathfrak{l}_r$ die r gemäss § 149 ausgewählten Primfactoren der Relativdiscriminante von K. Es bedeute nun A irgend eine Idealklasse in K, $\mathfrak{J}$ ein zu $\mathfrak{l}=(1-\zeta)$ und zur Relativdiscriminante von K primes Ideal der Klasse A und $\bar{\nu}=(N_k(\mathfrak{J}))^{hh^*}$ die nach der Vorschrift in § 149 (S. 462) aus $\mathfrak{J}$ gebildete und mit einem gewissen Einheitsfactor versehene ganze Zahl in $k(\zeta)$, so dass

$$\chi_1(\mathfrak{J})=\left\{\frac{\bar{\nu},\ \mu}{\mathfrak{l}_1}\right\},\quad\ldots,\quad\chi_r(\mathfrak{J})=\left\{\frac{\bar{\nu},\ \mu}{\mathfrak{l}_r}\right\}$$

die r Einzelcharaktere sind, welche das Geschlecht von $\mathfrak{J}$ bestimmen. Es sei $\mathfrak{p}$ ein Ideal des Kreiskörpers $k(\zeta)$, wofern es ein solches giebt, welches in $\bar{\nu}$ zu einem nicht durch l teilbaren Exponenten vorkommt; dabei ist $\mathfrak{p}$ sicher von $\mathfrak{l}$ verschieden und prim zur Relativdiscriminante von K. Da $N_k(\mathfrak{J})$ die Relativnorm eines Ideals ist, so muss $\mathfrak{p}$ im Körper K zerlegbar sein. Es gilt mithin nach Satz 149 (S. 398) für jedes solche Primideal $\mathfrak{p}$ die Gleichung $\left\{\frac{\mu}{\mathfrak{p}}\right\}=1$, und daher ist auch stets $\left\{\frac{\bar{\nu},\mu}{\mathfrak{p}}\right\}=1$. Mit Rücksicht auf Satz 163 (S. 490) folgt daher

$$\prod_{(\mathfrak{w})}\left\{\frac{\bar{\nu},\ \mu}{\mathfrak{w}}\right\}=1, \tag{153.}$$

wenn $\mathfrak{w}$ alle in der Relativdiscriminante von K enthaltenen, von $\mathfrak{l}$ verschiedenen Primideale und ausserdem das Primideal $\mathfrak{l}$ durchläuft. Ferner ist, wenn $\mathfrak{l}_{r+1}, \mathfrak{l}_{r+2}, \ldots, \mathfrak{l}_t$ die ausser $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_r$ in der Relativdiscriminante aufgehenden Primideale bedeuten, nach § 149

$$(154.)\quad \left\{\frac{\bar{\nu},\ \mu}{\mathfrak{l}_{r+1}}\right\}=1,\quad \left\{\frac{\bar{\nu},\ \mu}{\mathfrak{l}_{r+2}}\right\}=1,\quad \ldots,\quad \left\{\frac{\bar{\nu},\ \mu}{\mathfrak{l}_t}\right\}=1.$$

Kommt nun in der Relativdiscriminante des Körpers K das Primideal $\mathfrak{l}$ vor, so ist wegen (153.) schon hiermit bewiesen, dass das Product sämtlicher r Charaktere gleich 1 ist. Kommt andererseits das Primideal $\mathfrak{l}$ in jener Relativdiscriminante nicht vor, so ist nach Satz 150 (S. 402) die Zahl $\bar{\nu}$ Normenrest des Körpers K nach $\mathfrak{l}$, und folglich ist nach Satz 151 (S. 420) $\left\{\frac{\bar{\nu},\ \mu}{\mathfrak{l}}\right\}=1$; damit erkennen wir aus (153.) und (154.) auch in diesem Falle den einen Teil der Aussage des Satzes 164 als richtig.

Den Beweis für den anderen Teil der Aussage des Satzes 164 führen wir der Kürze wegen nur in dem Fall, dass die Relativdiscriminante des Körpers K den Primfactor $\mathfrak{l}$ nicht enthält. Es seien dann wiederum $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$ die t in der Relativdiscriminante von K aufgehenden Primideale des Körpers $k(\zeta)$, und $\lambda_1, \ldots, \lambda_t$ seien bezüglich Primärzahlen von $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$; ferner gehe allgemein $\mathfrak{l}_i$ in μ genau e_i mal auf, und es sei e_i^* dann eine ganze rationale Zahl mit der Congruenzeigenschaft $e_i e_i^* \equiv 1$ nach l. Endlich mögen $\gamma_1, \ldots, \gamma_r$ beliebig gewählte r der Bedingung $\gamma_1 \ldots \gamma_r = 1$ genügende $l$te Einheitswurzeln sein; nach Satz 152 (S. 426) giebt es dann stets in $k(\zeta)$ ein Primideal $\mathfrak{p}$, das in μ nicht aufgeht und überdies die Forderungen

$$(155.)\quad \left\{\frac{\lambda_1}{\mathfrak{p}}\right\}^m=\gamma_1^{e_1^*},\quad \left\{\frac{\lambda_2}{\mathfrak{p}}\right\}^m=\gamma_2^{e_2^*},\quad \ldots,\quad \left\{\frac{\lambda_r}{\mathfrak{p}}\right\}^m=\gamma_r^{e_r^*},$$

$$(156.)\quad \left\{\frac{\lambda_{r+1}}{\mathfrak{p}}\right\}^m=1,\quad \left\{\frac{\lambda_{r+2}}{\mathfrak{p}}\right\}^m=1,\quad \ldots,\quad \left\{\frac{\lambda_t}{\mathfrak{p}}\right\}^m=1$$

für irgend einen Exponenten m aus der Reihe $1, 2, \ldots, l-1$ erfüllt. Ist π eine Primärzahl von $\mathfrak{p}$, so folgt wegen (155.) mit Benutzung von Satz 161 (S. 471)

$$(157.)\quad \left\{\frac{\pi^m,\ \mu}{\mathfrak{l}_i}\right\}=\left\{\frac{\pi,\ \mu}{\mathfrak{l}_i}\right\}^m=\left\{\frac{\pi}{\mathfrak{l}_i}\right\}^{me_i}=\left\{\frac{\lambda_i}{\mathfrak{p}}\right\}^{me_i}=\gamma_i,$$
$$(i=1,\ 2,\ \ldots,\ r),$$

Ferner ergiebt sich wegen (156.) in ähnlicher Weise

$$(158.)\qquad \left\{\frac{\pi,\ \mu}{\mathfrak{l}_i}\right\} = \left\{\frac{\pi}{\mathfrak{l}_i}\right\}^{e_i} = \left\{\frac{\lambda_i}{\mathfrak{p}}\right\}^{e_i} = 1,$$

$$(i = r+1,\ r+2,\ \ldots,\ t).$$

Da $\gamma_1 \ldots \gamma_r = 1$ ist, so ist wegen (157.) und (158.)

$$(159.)\qquad \underset{(\mathfrak{w})}{\Pi}\left\{\frac{\pi,\ \mu}{\mathfrak{w}}\right\} = 1,$$

wenn hierin $\mathfrak{w}$ alle Primideale $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$ durchläuft. Bedeutet nun $\mathfrak{m}$ ein von $\mathfrak{p}, \mathfrak{l}_1, \ldots, \mathfrak{l}_t$ verschiedenes Primideal in $k(\zeta)$, so ist gemäss Satz 150 (S. 402) die Zahl π Normenrest des Kummer'schen Körpers K nach $\mathfrak{m}$ und folglich nach Satz 151 (S. 420) stets $\left\{\frac{\pi,\ \mu}{\mathfrak{m}}\right\} = 1$. Mit Rücksicht auf diesen Umstand und wegen (159.) lehrt der Satz 163 (S. 490), dass auch $\left\{\frac{\pi,\ \mu}{\mathfrak{p}}\right\} = 1$, d. h. $\left\{\frac{\mu}{\mathfrak{p}}\right\} = 1$ sein muss. Infolge der letzteren Gleichung zerfällt das Primideal $\mathfrak{p}$ nach Satz 149 (S. 398) im Körper K in l Primideale. Ist $\mathfrak{P}$ eines derselben, so hat, wenn wir (157.) und (158.) berücksichtigen, das Ideal $\mathfrak{P}^m$ offenbar die vorgeschriebenen Einheitswurzeln $\gamma_1, \ldots, \gamma_r$ als Charaktere, und damit ist der Satz 164 für den hier betrachteten Fall vollständig bewiesen.

Geht $\mathfrak{l}$ in der Relativdiscriminante von K auf, so hat man, um den Satz 164 zu beweisen, an den vorstehenden Ausführungen eine geeignete Abänderung anzubringen, die man leicht aus der Analogie mit den entsprechenden Betrachtungen für den quadratischen Körper (vergl. S. 312—314) ersieht.

Kummer hat seinen Untersuchungen einen gewissen Zahlenring im Körper $K = k(\sqrt[l]{\mu}, \zeta)$, nicht die Gesamtheit der ganzen Zahlen dieses Körpers zu Grunde gelegt. Der Begriff des Geschlechtes bedarf dann einer gewissen veränderten Fassung. Es ist *Kummer*'s grosses Verdienst, für den von ihm ausgewählten Zahlenring diejenige Thatsache aufgestellt und bewiesen zu haben, die für den Körper K selbst sich in dem Satze 164 ausdrückt. [*Kummer*[20].] Ausser dem von Kummer behandelten Ringe sind noch unendlich viele andere Ringe in K vorhanden, deren Theorie mit entsprechendem Erfolge zu entwickeln sein würde.

§ 164.

Die Klassen des Hauptgeschlechtes in einem regulären Kummer'schen Körper.

Wir heben in diesem und dem nächsten Paragraphen einige wichtige Folgerungen hervor, die aus dem Fundamentalsatz 164 für den Kummer'schen Körper $K = k(\sqrt[l]{\mu}, \zeta)$ sich ergeben, und die den in § 71 und § 72 oder in § 82 für den quadratischen Körper entwickelten Sätzen entsprechen.

Satz 165. Die Anzahl g der Geschlechter in einem regulären Kummer'schen Körper ist gleich der Anzahl seiner ambigen Complexe.

Beweis. Wenn t und n die Bedeutung wie in Satz 159 (S. 459) haben, und wenn wir berücksichtigen, dass nach Satz 164 (S. 492) $g = l^{r-1}$ ist, so folgt aus Hülfssatz 34 (S. 468) $r-1 \leqq t+n-\frac{l+1}{2}$, und da nach Hülfssatz 33 (S. 466) andererseits $t+n-\frac{l+1}{2} \leqq r-1$ sein muss, so folgt

$$r-1 = t+n-\frac{l+1}{2}.$$

Die im Beweise (S. 469) zu Hülfssatz 34 bestimmte Anzahl a der ambigen Complexe ist mithin $= l^{r-1}$; wir haben daher $a = g$.

Satz 166. *Jeder Complex des Hauptgeschlechtes in einem regulären Kummer'schen Körper K ist die* $(1-S)$*te symbolische Potenz eines Complexes in K, d. h. jede Klasse des Hauptgeschlechtes in einem regulären Kummer'schen Körper K ist gleich dem Product aus der* $(1-S)$*ten symbolischen Potenz einer Klasse und aus einer solchen Klasse, welche Ideale des Kreiskörpers* $k(\zeta)$ *enthält.*

Beweis. In dem Beweise (S. 469) zu Hülfssatz 34 ist die Gleichung $af' = gf$ abgeleitet; hierbei bedeutet a die Anzahl der ambigen Complexe, f' die Anzahl derjenigen Complexe, welche gleich $(1-S)$ten symbolischen Potenzen von Complexen sind, ferner bedeutet g die Anzahl der Geschlechter und f die Anzahl der Complexe des Hauptgeschlechtes. Da nach Satz 165 $a = g$ ist, so folgt $f' = f$, und damit ist bewiesen, dass jeder Complex des Hauptgeschlechtes die $(1-S)$te symbolische Potenz eines Complexes ist.

§ 165.

Der Satz von den Relativnormen der Zahlen eines regulären Kummer'schen Körpers.

Satz 167. *Wenn ν, μ zwei ganze Zahlen des regulären Kreiskörpers $k(\zeta)$ bedeuten, von denen μ nicht die $l$te Potenz einer ganzen Zahl in $k(\zeta)$ ist, und welche für jedes Primideal $\mathfrak{w}$ in $k(\zeta)$ die Bedingung*

$$\left\{\frac{\nu,\ \mu}{\mathfrak{w}}\right\} = 1$$

erfüllen, so ist die Zahl ν stets gleich der Relativnorm einer ganzen oder gebrochenen Zahl A des Kummer'schen Körpers $K = k(\sqrt[l]{\mu}, \zeta)$.

Beweis. Wir beweisen diesen Satz zunächst für den Fall, dass ν eine Einheit in $k(\zeta)$ ist. Es mögen wiederum t und n für den Kummer'schen Körper $K = k(\sqrt[l]{\mu}, \zeta)$ die Bedeutung wie in Satz 159 (S. 459) haben; im Beweise zu Satz 165 ist gezeigt worden, dass $r - 1 = t + n - \frac{l+1}{2}$ sein muss, d. h. es ist $n = \frac{l-1}{2} - t + r$. Andererseits betrachten wir die $r^* = t - r$ Einheiten $\varepsilon_1, \ldots, \varepsilon_{r^*}$, die in § 149 (S. 464) bestimmt worden sind. Wegen der Gleichungen (140.) (S. 464) kann ein Product aus Potenzen dieser r^* Einheiten nur dann die $l$te Potenz einer Einheit in $k(\zeta)$ sein, wenn die Potenzexponenten sämtlich durch l teilbar sind. Es müssen sich daher, da die Gesamtheit aller Einheiten in $k(\zeta)$ eine Schar vom Grade $\frac{l-1}{2}$ bildet, weiter $\frac{l-1}{2} - r^*$ Einheiten $\varepsilon_{r^*+1}, \varepsilon_{r^*+2}, \ldots, \varepsilon_{\frac{l-1}{2}}$ in $k(\zeta)$ bestimmen lassen, so dass überhaupt jede Einheit ξ in $k(\zeta)$ sich in der Gestalt

$$\xi = \varepsilon_1^{x_1} \varepsilon_2^{x_2} \ldots \varepsilon_{\frac{l-1}{2}}^{x_{\frac{l-1}{2}}} \varepsilon^l$$

darstellen lässt, wobei $x_1, x_2, \ldots, x_{\frac{l-1}{2}}$ ganze rationale Exponenten sind und ε eine geeignete Einheit in $k(\zeta)$ bedeutet. Setzen wir nun allgemein

$$\left\{\frac{\varepsilon_u,\ \mu}{\mathfrak{l}_{t-v+1}}\right\} = \zeta^{e_{uv}},$$

$$\left(u = 1, 2, \ldots, \frac{l-1}{2};\ v = 1, 2, \ldots, r^*\right)$$

so liefern die r^* Gleichungen

$$(160.)\quad \left\{\frac{\xi,\ \mu}{\mathfrak{l}_t}\right\}=1,\quad \left\{\frac{\xi,\ \mu}{\mathfrak{l}_{t-1}}\right\}=1,\quad \ldots,\quad \left\{\frac{\xi,\ \mu}{\mathfrak{l}_{t-r^*+1}}\right\}=1$$

für die Exponenten $x_1, x_2, \ldots, x_{\frac{l-1}{2}}$ die r^* linearen Congruenzen

$$(161.)\quad \left\{\begin{array}{l} e_{11}x_1+e_{21}x_2+\cdots+e_{\frac{l-1}{2},1}\,x_{\frac{l-1}{2}}\equiv 0, \\ \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot \\ e_{1r^*}x_1+e_{2r^*}x_2+\cdots+e_{\frac{l-1}{2},r^*}\,x_{\frac{l-1}{2}}\equiv 0, \end{array}\right\}(l).$$

Wegen (140.) (S. 464) haben wir

$$\left.\begin{array}{lllll} e_{11}\equiv 1, & e_{21}\equiv 0, & e_{31}\equiv 0, & \ldots, & e_{r^*1}\equiv 0, \\ & e_{22}\equiv 1, & e_{32}\equiv 0, & \ldots, & e_{r^*2}\equiv 0, \\ & & e_{33}\equiv 1, & \ldots, & e_{r^*3}\equiv 0, \\ & & \cdot\quad\cdot\quad\cdot & \cdot\quad\cdot\quad\cdot & \cdot\quad\cdot\quad\cdot \\ & & & & e_{r^*,r^*}\equiv 1, \end{array}\right\}(l);$$

und daher sind die r^* linearen Congruenzen (161.) von einander unabhängig; es folgt somit, dass alle diejenigen Einheiten ξ, welche den Bedingungen (160.) genügen, eine Einheitenschar vom Grade

$$\frac{l-1}{2}-r^*=\frac{l-1}{2}-t+r$$

bilden.

Wir haben nun zu Beginn dieses Beweises festgestellt, dass der Grad n der Schar aller derjenigen Einheiten in $k(\zeta)$, welche Relativnormen von Einheiten oder gebrochenen Zahlen in K sind, den gleichen Wert besitzt. Da ferner jede Einheit in $k(\zeta)$, welche die Relativnorm einer Einheit oder einer gebrochenen Zahl im Kummer'schen Körper K ist, offenbar Normenrest von K nach $\mathfrak{l}$ sein und daher nach Satz 151 (S. 420) notwendig auch den Gleichungen (160.) genügen muss, so gehört jede Einheit der zu Anfang behandelten Schar auch der zweiten Einheitenschar an; weil beide Einheitenscharen gleiche Grade haben, sind sie mit einander identisch. Die vorgelegte Einheit ν genügt nun nach Voraussetzung den Bedingungen (160.) und gehört also der zweiten Einheitenschar an; nach dem eben Bewiesenen ist mithin ν auch in der zuerst behandelten Einheitenschar enthalten, d. h. es ist ν gleich der Relativnorm einer Einheit oder einer gebrochenen Zahl in K.

Es sei jetzt ν eine beliebige ganze Zahl in K, welche die Voraussetzung des Satzes 167 erfüllt; wir fassen die in ν aufgehenden Primideale des Körpers $k(\zeta)$ in's Auge. Wir setzen $\lambda = 1-\zeta$ und $\mathfrak{l} = (\lambda)$. Kommt das Primideal $\mathfrak{l}$ des Körpers $k(\zeta)$ in ν zu einer Potenz erhoben vor, deren Exponent b nicht durch l teilbar ist, und geht ausserdem $\mathfrak{l}$ in der Relativdiscriminante des Körpers K nicht auf, so haben wir auf Grund der Angaben am Schlusse von § 133 auf S. 423.

$$\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\} = \left\{\frac{\lambda^b,\ \mu}{\mathfrak{l}}\right\} = \left\{\frac{\mu}{\mathfrak{l}}\right\}^{-b},$$

und mit Rücksicht auf die hieraus zu entnehmende Gleichung

$$\left\{\frac{\mu}{\mathfrak{l}}\right\} = 1$$

ist $\mathfrak{l}$ nach Satz 149 (S. 398) in K als Product von l Primfactoren darstellbar. Bedeutet $\mathfrak{L}$ einen derselben, so haben wir $\mathfrak{l} = N_k(\mathfrak{L})$.

Es sei ferner $\mathfrak{p}$ ein von $\mathfrak{l}$ verschiedenes Primideal des Kreiskörpers $k(\zeta)$, und es komme $\mathfrak{p}$ in ν zu einer Potenz erhoben vor, deren Exponent b nicht durch l teilbar ist; dagegen sei der Exponent a, zu dem $\mathfrak{p}$ in μ aufgeht, durch l teilbar: dann ist nach der Definition des Symbols

$$\left\{\frac{\nu,\ \mu}{\mathfrak{p}}\right\} = \left\{\frac{\mu^b}{\mathfrak{p}}\right\}^{-1},$$

und hieraus folgt wegen der Voraussetzung des Satzes 167 $\left\{\frac{\mu}{\mathfrak{p}}\right\} = 1$; nach Satz 149 (S. 398) ist also $\mathfrak{p}$ in K als Product von l Primidealen darstellbar. Ist $\mathfrak{P}$ eines dieser l Primideale, so wird $\mathfrak{p} = N_k(\mathfrak{P})$.

Endlich sind die in der Relativdiscriminante von K aufgehenden Primideale des Körpers $k(\zeta)$ stets $l$te Potenzen von Primidealen in K und daher ebenfalls Relativnormen von Idealen in K. Aus allen diesen Umständen zusammengenommen folgt, dass ν die Relativnorm eines Ideals $\mathfrak{H}$ in K sein muss, d. h. es ist $\nu = N_k(\mathfrak{H})$.

Wegen der Voraussetzung des Satzes 167 gehört ferner $\mathfrak{H}$ dem Hauptgeschlecht in K an, und wir können daher nach Satz 166 (S. 495)

$$\mathfrak{H} \sim \mathfrak{j}\mathfrak{J}^{1-S}$$

setzen, in solcher Weise, dass $\mathfrak{j}$ ein Ideal in $k(\zeta)$ und $\mathfrak{J}$ ein Ideal in K bedeutet. Ist h die Anzahl der Idealklassen in $k(\zeta)$, so haben wir

$\mathfrak{j}^h \sim 1$, und folglich muss $A = \left(\frac{\mathfrak{H}}{\mathfrak{J}^{1-S}}\right)^h$ eine ganze oder gebrochene Zahl des Körpers K sein; die Relativnorm dieser Zahl $N_k(A)$ ist offenbar $= \varepsilon \nu^h$, wo ε eine Einheit in $k(\zeta)$ bedeutet. Aus der letzten Gleichung folgt nach Satz 151 (S. 420), dass für jedes beliebige Primideal $\mathfrak{w}$ in $k(\zeta)$ notwendig $\left\{\frac{\varepsilon \nu^h, \mu}{\mathfrak{w}}\right\} = 1$ und daher auch $\left\{\frac{\varepsilon, \mu}{\mathfrak{w}}\right\} = 1$ sein muss. Es ist nun im ersten Teile des gegenwärtigen Beweises gezeigt worden, dass unter diesen Umständen ε stets gleich der Relativnorm einer Zahl in K sein muss; wir setzen $\varepsilon = N_k(H)$, wo H eine Zahl in K ist. Bedeuten dann b und e zwei ganze rationale Zahlen von der Art, dass $bh + el = 1$ ist, so folgt

$$\nu = N_k(A^b H^{-b} \nu^e),$$

und hiermit ist der Beweis für den Satz 167 vollständig erbracht.

In diesem Beweise können wir die Anwendung des Satzes 151 beidemal auf den Fall $\mathfrak{w} \neq \mathfrak{l}$ beschränken, da dann nach Satz 163 (S. 490) die behaupteten Thatsachen auch für $\mathfrak{w} = \mathfrak{l}$ folgen.

Damit ist es dann gelungen, alle diejenigen Eigenschaften auf den regulären Kummer'schen Körper zu übertragen, welche für den quadratischen Körper bereits von *Gauss* aufgestellt und bewiesen worden sind.

Capitel XXXV.

Neue Begründung der Theorie des regulären Kummer'schen Körpers.

§ 166.

Die wesentlichen Eigenschaften der Einheiten des regulären Kreiskörpers.

Wir haben gesehen, eine wie wichtige Rolle das besondere Symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ in der Theorie des Kummer'schen Körpers spielt. Was die Definition dieses Symbols in § 131 (S. 413) und die Ableitung seiner Eigenschaften in § 131 bis § 133 betrifft, so knüpften wir in der dortigen Darstellung an die von *Kummer* eingeführten logarithmischen Differentialquotienten der zu einer Zahl $\omega \equiv 1$ nach $\mathfrak{l}$ gehörenden Function

$\omega(x)$ an. Die in § 131 bis § 133 für das Symbol $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}$ im Kummer'schen Körper ausgeführten Rechnungen entsprechen übrigens genau denjenigen Betrachtungen, welche in § 64 für das Symbol $\left(\frac{n,m}{2}\right)$ im quadratischen Körper angestellt worden sind. Obwohl es nun bereits gelang, die von *Kummer* ersonnenen rechnerischen Hülfsmittel auf ein geringes Mass zu bringen, so erscheint es mir doch noch, vor allem auch im Hinblick auf eine künftige Erweiterung der Theorie, notwendig zu untersuchen, ob nicht eine Begründung der Theorie des Kummer'schen Körpers ganz ohne jene Rechnungen möglich ist. Ich gebe in diesem Capitel den Weg hierzu kurz an.

Zunächst können leicht ohne Rechnung und ohne Heranziehung der Bernoulli'schen Zahlen die späterhin wesentlichen Eigenschaften der Einheiten des regulären Kreiskörpers $k(\zeta)$ abgeleitet werden. Für Satz 156 erinnern wir uns des zweiten auf S. 440 mitgeteilten Beweises.

Wir können dann aus diesem Satz 156 den Satz 155 (S. 438) wie folgt ableiten. Wir wollen unter $\varepsilon_1, \ldots, \varepsilon_{l^*}$ irgend ein System von l^* reellen Grundeinheiten des Körpers $k(\zeta)$ verstehen; wir bestimmen dann positive Exponenten $e_1, \ldots, e_{l^*}$ und gewisse ganze rationale, zu l prime Zahlen $a_1, \ldots, a_{l^*}, b_1, \ldots, b_{l^*}$ derart, dass die Congruenzen

$$\varepsilon_1 \equiv a_1 + b_1\lambda^{e_1}, \qquad (\mathfrak{l}^{e_1+1}),$$
$$\cdots\cdots\cdots\cdots$$
$$\varepsilon_{l^*} \equiv a_{l^*} + b_{l^*}\lambda^{e_{l^*}}, \qquad (\mathfrak{l}^{e_{l^*}+1})$$

gültig sind. Wir nehmen an, es habe unter den Exponenten $e_1, \ldots, e_{l^*}$ etwa e_1 den niedrigsten vorkommenden Wert. Dann können wir, wie leicht ersichtlich ist, die l^*-1 Einheiten $\varepsilon_2, \ldots, \varepsilon_{l^*}$ derart mit Potenzen von ε_1 multipliciren, dass für die l^*-1 entstehenden Producte $\varepsilon'_2, \ldots, \varepsilon'_{l^*}$ die Congruenzen

$$\varepsilon'_2 = \varepsilon_2\varepsilon_1^{f_2} = a'_2 + b'_2\lambda^{e'_2}, \qquad (\mathfrak{l}^{e'_2+1}),$$
$$\cdots\cdots\cdots\cdots$$
$$\varepsilon'_{l^*} = \varepsilon_{l^*}\varepsilon_1^{f_{l^*}} \equiv a'_{l^*} + b'_{l^*}\lambda^{e'_{l^*}}, \qquad (\mathfrak{l}^{e'_{l^*}+1})$$

bestehen, wo $a'_2, \ldots, a'_{l^*}, b'_2, \ldots, b'_{l^*}$ ganze rationale, zu l prime Zahlen bedeuten, und wo nun die Exponenten $e'_2, \ldots, e'_{l^*}$ sämtlich grösser als e_1 sind. Die Einheiten $\varepsilon_1, \varepsilon'_2, \varepsilon'_3, \ldots, \varepsilon'_{l^*}$ bilden wiederum

ein System von Grundeinheiten in $k(\zeta)$. Nun möge unter den Exponenten e_2', ..., e_{l^*}' etwa e_2' den niedrigsten vorkommenden Wert haben; dann ist es weiter möglich, die Einheiten ε_3', ..., ε_{l^*}' derart mit Potenzen von ε_2' zu multipliciren, dass für die l^*-2 entstehenden Producte ε_3'', ..., ε_{l^*}'' die Congruenzen

$$\varepsilon_3'' = \varepsilon_3' \varepsilon_2'^{f_3'} \equiv a_3'' + b_3'' \lambda^{e_3''}, \qquad (\mathfrak{l}^{e_3''+1}),$$

$$\cdots\cdots\cdots\cdots$$

$$\varepsilon_{l^*}'' = \varepsilon_{l^*}' \varepsilon_2'^{f_{l^*}'} \equiv a_{l^*}'' + b_{l^*}'' \lambda^{e_{l^*}''}, \qquad (\mathfrak{l}^{e_{l^*}''+1})$$

gelten, wo a_3'', ..., a_{l^*}'', b_3'', ..., b_{l^*}'' ganze rationale, zu l prime Zahlen bedeuten und nunmehr die Exponenten e_3'', ..., e_{l^*}'' sämtlich grösser als e_2' sind. Die Einheiten ε_1, ε_2', ε_3'', ε_4'', ..., ε_{l^*}'' bilden offenbar wiederum ein System von Grundeinheiten in $k(\zeta)$. Indem wir in geeigneter Weise fortfahren, gelangen wir zu einem System von Grundeinheiten ε_1, ε_2', ..., $\varepsilon_{l^*}^{(l^*-1)}$ in $k(\zeta)$, die den Congruenzen

$$\varepsilon_1 \equiv a_1 + b_1 \lambda^{e_1}, \qquad (\mathfrak{l}^{e_1+1}),$$

$$\varepsilon_2' \equiv a_2' + b_2' \lambda^{e_2'}, \qquad (\mathfrak{l}^{e_2'+1}),$$

$$\varepsilon_3'' \equiv a_3'' + b_3'' \lambda^{e_3''}, \qquad (\mathfrak{l}^{e_3''+1}),$$

$$\cdots\cdots\cdots\cdots$$

$$\varepsilon_{l^*}^{(l^*-1)} \equiv a_{l^*}^{(l^*-1)} + b_{l^*}^{(l^*-1)} \lambda^{e_{l^*}^{(l^*-1)}}, \quad (\mathfrak{l}^{e_{l^*}^{(l^*-1)}+1})$$

genügen, wo a_1, ..., $a_{l^*}^{(l^*-1)}$, b_1, ..., $b_{l^*}^{(l^*-1)}$ ganze rationale, zu l prime Zahlen sind, während für die Exponenten e_1, ..., $e_{l^*}^{(l^*-1)}$ die Kette von Ungleichungen

$$(162.) \qquad e_1 < e_2' < e_3'' < \cdots < e_{l^*}^{(l^*-1)}$$

gilt. Da die betrachteten Einheiten sämtlich reell sind, so fallen die Exponenten e_1, e_2', e_3'', ..., $e_{l^*}^{(l^*-1)}$ gerade aus. Wäre nun

$$e_{l^*}^{(l^*-1)} \geqq l-1,$$

so würde nach Satz 156 $\varepsilon_{l^*}^{(l^*-1)}$ die $l$te Potenz einer Einheit η in $k(\zeta)$ sein. Drücken wir dann η durch die Einheiten ζ, ε_1, ε_2', ..., $\varepsilon_{l^*}^{(l^*-1)}$ aus in der Gestalt

$$\eta = \zeta^u \varepsilon_1^{u_1} \varepsilon_2'^{u_2} \ldots (\varepsilon_{l^*}^{(l^*-1)})^{u_{l^*}},$$

wo $u, u_1, u_2, \ldots, u_{l^*}$ ganze rationale Exponenten sind, und erheben diese Gleichung in die $l$te Potenz, so erhalten wir eine Relation zwischen den l^* Einheiten $\varepsilon_1, \varepsilon_2', \ldots, \varepsilon_{l^*}^{(l^*-1)}$ mit Exponenten, die nicht sämtlich Null sind; dies widerspricht der Thatsache, dass $\varepsilon_1, \varepsilon_2', \ldots, \varepsilon_{l^*}^{(l^*-1)}$ ein System von Grundeinheiten in $k(\zeta)$ bilden. Es ist daher

$$e_{l^*}^{(l-1)} < l-1.$$

Hieraus folgt mit Rücksicht auf die Ungleichungen (162.), dass notwendigerweise

$$e_1 = 2, \quad e_2' = 4, \quad e_3'' = 6, \quad \ldots, \quad e_{l^*}^{(l^*-1)} = l-3$$

sein muss, und diese Thatsache lässt unmittelbar auf das Vorhandensein von solchen Einheiten $\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_{l^*}$ schliessen, die von der im Satze 155 (S. 438) verlangten Beschaffenheit sind.

Der Satz 157 (S. 441) folgt wie in § 142 aus Satz 155.

§ 167.

Beweis einer Eigenschaft für die Primärzahlen von Primidealen der zweiten Art.

Wir legen die in § 131 (S. 411) gegebene Definition des Symbols $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$ für ein Primideal $\mathfrak{w} \neq \mathfrak{l}$ zu Grunde, sehen jedoch vorläufig von einer Definition des Symbols $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ ab; wir benutzen dementsprechend die Sätze 150 (S. 402), 151 (S. 420) ebenfalls nur für $\mathfrak{w} \neq \mathfrak{l}$. Die Sätze 158 (S. 449), 159 (S. 459) folgen dann unmittelbar in der dort dargelegten Weise für den Kummer'schen Körper $k(\sqrt[l]{\mu}, \zeta)$, sobald wir die einschränkende Annahme machen, dass die Relativdiscriminante von $k(\sqrt[l]{\mu}, \zeta)$ in Bezug auf $k(\zeta)$ zu $\mathfrak{l}$ prim sei. Unter derselben Einschränkung gelangen wir ohne Gebrauch des Symbols $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ zu dem Begriff des Charakters eines Ideals in $k(\sqrt[l]{\mu}, \zeta)$, zu der Einteilung der Idealklassen eines Kummer'schen Körpers in Geschlechter, sowie zu der Gültigkeit der Hülfssätze 33 (S. 466), 34 (S. 468), 35 (S. 470) und beweisen dann zunächst folgenden Hülfssatz:

Hülfssatz 43. Eine jede Primärzahl $\varkappa$ eines Primideals $\mathfrak{q}$ der

zweiten Art ist der $l$ten Potenz einer ganzen Zahl in $k(\zeta)$ nach $\mathfrak{l}^l$ congruent.

Beweis. Es seien $\varepsilon_1, \ldots, \varepsilon_{l^*}$ die in § 166 bestimmten und dort mit $\varepsilon_1, \ldots, \varepsilon_{l^*}^{(l^*-1)}$ bezeichneten $l^* = \frac{l-3}{2}$ Grundeinheiten des Körpers $k(\zeta)$; es seien ferner $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$ von $\mathfrak{l}$ verschiedene Primideale in $k(\zeta)$ von der Beschaffenheit, dass

$$(163.)\quad \begin{cases} \left\{\frac{\zeta}{\mathfrak{p}}\right\} = \zeta^*, & \left\{\frac{\varepsilon_1}{\mathfrak{p}}\right\} = 1, \quad \left\{\frac{\varepsilon_2}{\mathfrak{p}}\right\} = 1, \quad \ldots, \quad \left\{\frac{\varepsilon_{l^*}}{\mathfrak{p}}\right\} = 1, \\ \left\{\frac{\zeta}{\mathfrak{p}_1}\right\} = 1, & \left\{\frac{\varepsilon_1}{\mathfrak{p}_1}\right\} = \zeta_1, \quad \left\{\frac{\varepsilon_2}{\mathfrak{p}_1}\right\} = 1, \quad \ldots, \quad \left\{\frac{\varepsilon_{l^*}}{\mathfrak{p}_1}\right\} = 1, \\ \cdots & \cdots \\ \left\{\frac{\zeta}{\mathfrak{p}_{l^*}}\right\} = 1, & \left\{\frac{\varepsilon_1}{\mathfrak{p}_{l^*}}\right\} = 1, \quad \left\{\frac{\varepsilon_2}{\mathfrak{p}_{l^*}}\right\} = 1, \quad \ldots, \quad \left\{\frac{\varepsilon_{l^*}}{\mathfrak{p}_{l^*}}\right\} = \zeta_{l^*} \end{cases}$$

ausfällt, wo $\zeta^*, \zeta_1, \ldots, \zeta_{l^*}$ irgend welche von 1 verschiedene $l$te Einheitswurzeln bedeuten. Die Existenz solcher Primideale folgt aus Satz 152 (S. 426); wenn wir auf den Beweis dieses Satzes zurückgreifen, sehen wir, dass nicht bloss die Anzahl, sondern die Summe der reciproken Normen aller Primideale $\mathfrak{r}$ von der dort angegebenen Beschaffenheit unendlich war, und wegen dieses Umstandes dürfen wir, wie aus den Betrachtungen beim Beweise des Satzes 83 (S. 264) ersichtlich ist, gegenwärtig annehmen, dass die Primideale $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$ obenein sämtlich vom ersten Grade sind. Ferner können wir voraussetzen, dass die durch $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$ teilbaren rationalen Primzahlen sämtlich voneinander verschieden ausfallen. Es seien $\pi, \pi_1, \ldots, \pi_{l^*}$ Primärzahlen bez. von $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$.

Wir behandeln nun die Annahme, es gäbe l^*+1 ganze, nicht sämtlich durch l teilbare Exponenten $u, u_1, \ldots, u_{l^*}$, für welche der Ausdruck $\alpha = \pi^u \pi_1^{u_1} \ldots \pi_{l^*}^{u_{l^*}}$ der $l$ten Potenz einer ganzen Zahl in $k(\zeta)$ nach $\mathfrak{l}^l$ congruent wird. Nach Satz 148 (S. 393) besitzt dann die Relativdiscriminante des Kummer'schen Körpers $k(\sqrt[l]{\alpha}, \zeta)$ eine gewisse Anzahl t der Primideale $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$, aber nicht das Primideal $\mathfrak{l}$ als Factor. Andererseits folgt aus (163.) unter Berücksichtigung des Satzes 151 (S. 420), dass der Grad m der Schar derjenigen Einheiten in $k(\zeta)$, welche Relativ-

normen von Einheiten in $k(\sqrt[l]{\alpha}, \zeta)$ sind, höchstens den Wert $\frac{l-1}{2}-t$ hat; somit würde für den Kummer'schen Körper $k(\sqrt[l]{\alpha}, \zeta)$

$$m \leqq \frac{l-1}{2}-t, \quad \text{d. h.} \quad t+m-\frac{l+1}{2}<0$$

ausfallen, was nach Satz 158 (S. 449) nicht sein kann. Damit ist die oben versuchte Annahme als unmöglich erkannt, d. h. für Exponenten $u, u_1, \ldots, u_{l^*}$, die nicht sämtlich durch l teilbar sind, ist der Ausdruck $\pi^u \pi_1^{u_1} \ldots \pi_{l^*}^{u_{l^*}}$ niemals der $l$ten Potenz einer ganzen Zahl in $k(\zeta)$ nach $\mathfrak{l}^l$ congruent.

Es sei $\varkappa$ eine Primärzahl des Primideals $\mathfrak{q}$. Aus dem Beweise des Satzes 157 (S. 441) entnehmen wir, dass es genau $\frac{(l-1).l^{l-3}}{l^{l^*}}$ nach $\mathfrak{l}^{l-1}$ und also $(l-1)l^{l^*+1}$ nach $\mathfrak{l}^l$ incongruente primäre Zahlen in $k(\zeta)$ giebt; andererseits ist die $l$te Potenz einer zu $\mathfrak{l}$ primen Zahl in $k(\zeta)$ stets der $l$ten Potenz einer der $l-1$ Zahlen $1, 2, \ldots, l-1$ nach $\mathfrak{l}^l$ congruent. Aus der vorhin gefundenen Thatsache folgt daher, dass es stets möglich sein muss, die Exponenten $u, u_1, \ldots, u_{l^*}$ derart zu bestimmen, dass der Ausdruck $\mu = \pi^u \pi_1^{u_1} \ldots \pi_{l^*}^{u_{l^*}} \varkappa$ der $l$ten Potenz einer ganzen Zahl in $k(\zeta)$ nach $\mathfrak{l}^l$ congruent wird; wir setzen, wenn $u, u_1, \ldots, u_{l^*}$ solcher Art bestimmt sind, $\alpha = \pi^u \pi_1^{u_1} \ldots \pi_{l^*}^{u_{l^*}}$, so dass $\mu = \alpha\varkappa$ wird, und behandeln nun die Annahme, dass eine gewisse positive Anzahl a von diesen Exponenten $u, u_1, \ldots, u_{l^*}$ zu l prim, die übrigen $\frac{l-1}{2}-a$ aber durch l teilbar seien. Es wäre dann wegen (163.) für den Kummer'schen Körper $k(\sqrt[l]{\mu}, \zeta)$, indem wir für ihn die Bezeichnungen des § 149 benutzen, $t = a+1$, $r^* = a$, $r = t - r^* = 1$, und folglich sind nach Hülfssatz 35 (S. 470) in diesem Körper $k(\sqrt[l]{\mu}, \zeta)$ alle Idealklassen vom Hauptgeschlecht. Hieraus ergiebt sich unmittelbar folgende Thatsache: wenn $\mathfrak{r}$ irgend ein Primideal in $k(\zeta)$ mit der Eigenschaft $\left\{\frac{\mu}{\mathfrak{r}}\right\} = 1$ ist und ϱ eine Primärzahl von $\mathfrak{r}$ bedeutet, so muss bei geeigneter Wahl der Einheit ξ das Charakterensystem der Zahl $\xi\varrho$ im Körper $k(\sqrt[l]{\mu}, \zeta)$

aus lauter Einheiten 1 bestehen; es ist also insbesondere

$$\left\{\frac{\xi\varrho,\,\mu}{\mathfrak{q}}\right\}=\left\{\frac{\xi\varrho}{\mathfrak{q}}\right\}=1,$$

und da $\mathfrak{q}$ ein Primideal zweiter Art sein soll, so ist auch $\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}=1$.

Wir bezeichnen jetzt die zu $\mathfrak{q}$ conjugirten und von $\mathfrak{q}$ verschiedenen Primideale mit $\mathfrak{q}'$, $\mathfrak{q}''$, ... und diejenigen Substitutionen aus der Gruppe von $k(\zeta)$, welche $\mathfrak{q}$ in $\mathfrak{q}'$, $\mathfrak{q}''$, ... überführen, bez. mit s', s'', ... Haben dann h, h^* die Bedeutung wie in § 149, und ist q die durch $\mathfrak{q}$ teilbare ganze rationale Primzahl, so ergiebt sich (ähnlich wie in § 158) mit Rücksicht auf die Bemerkung hinter dem Satze 157 (S. 441)

$$\varkappa(s'\varkappa)(s''\varkappa)\cdots=\varepsilon^l q^{hh^*},$$

wo ε eine Einheit in $k(\zeta)$ ist. Wegen unserer Annahme über die Exponenten $u, u_1, \ldots, u_{l^*}$, und da die Primideale $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$ vom ersten Grade und ferner die durch sie teilbaren rationalen Primzahlen unter sich verschieden sind, können wir aus dem Satz 152 (S. 426) schliessen, dass es in $k(\zeta)$ ein Primideal $\mathfrak{r}$ giebt mit den Eigenschaften

$$(164.)\quad \left\{\begin{array}{ll} \left\{\frac{\alpha}{\mathfrak{r}}\right\}=\zeta^{*-1}, & \left\{\frac{\varkappa}{\mathfrak{r}}\right\}=\zeta^{*}, \\ \left\{\frac{s'\alpha}{\mathfrak{r}}\right\}=1, & \left\{\frac{s'\varkappa}{\mathfrak{r}}\right\}=1, \\ \left\{\frac{s''\alpha}{\mathfrak{r}}\right\}=1, & \left\{\frac{s''\varkappa}{\mathfrak{r}}\right\}=1, \\ \cdots & \cdots \end{array}\right.$$

wo ζ^* irgend eine von 1 verschiedene $l$te Einheitswurzel bedeutet. Diese Gleichungen (164.) ergeben sofort

$$(165.)\quad \left\{\frac{\mu}{\mathfrak{r}}\right\}=1,\quad \left\{\frac{s'\mu}{\mathfrak{r}}\right\}=1,\quad \left\{\frac{s''\mu}{\mathfrak{r}}\right\}=1,\quad \ldots,$$

$$(166.)\quad \left\{\frac{\varkappa . s'\varkappa . s''\varkappa \ldots}{\mathfrak{r}}\right\}=\left\{\frac{q}{\mathfrak{r}}\right\}=\zeta^{*};$$

aus der ersten von den Gleichungen (165.) folgt nach dem zuvor Bewiesenen $\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}=1$, und in gleicher Weise liefern die weiteren Gleichungen (165.) die Beziehungen $\left\{\frac{\mathfrak{r}}{\mathfrak{q}'}\right\}=1$, $\left\{\frac{\mathfrak{r}}{\mathfrak{q}''}\right\}=1$, ...; durch Multi-

plication wird hieraus $\left\{\frac{\mathfrak{r}}{q}\right\}=1$, was wegen Satz 140 (S. 369) der Gleichung (166.) widerspricht. Unsere augenblicklich behandelte Annahme über die Exponenten $u, u_1, \ldots, u_{l^*}$ ist daher unzutreffend, d. h. diese Exponenten, wie sie oben bestimmt wurden, müssen sämtlich durch l teilbar sein, und α ist mithin gleich der $l$ten Potenz einer ganzen Zahl in $k(\zeta)$; hieraus ergiebt sich, dass $\varkappa$ congruent der $l$ten Potenz einer ganzen Zahl in $k(\zeta)$ nach $\mathfrak{l}^l$ ausfällt, womit der Hülfssatz 43 bewiesen ist.

§ 168.

Beweis des Reciprocitätsgesetzes für die Fälle, dass eines der beiden Primideale von der zweiten Art ist.

Wir gelangen jetzt schrittweise, wie folgt, zu einzelnen Teilen des Reciprocitätsgesetzes für $l$te Potenzreste:

Hülfssatz 44. Es sei $\mathfrak{q}$ ein Primideal zweiter Art und $\mathfrak{r}$ ein Primideal erster oder zweiter Art in $k(\zeta)$; wenn dann $\left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}=1$ ist, so wird auch $\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}=1$.

Beweis. Es seien $\varkappa$, ϱ Primärzahlen der Primideale $\mathfrak{q}$ bez. $\mathfrak{r}$. Mit Rücksicht auf Hülfssatz 43 (S. 502) besitzt die Relativdiscriminante des Körpers $k(\sqrt[l]{\varkappa}, \zeta)$ nach Satz 148 (S. 393) nur den einen Primfactor $\mathfrak{q}$, und daher gehören wegen des Hülfssatzes 35 (S. 470) in diesem Körper alle Ideale dem Hauptgeschlechte an. Wegen $\left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}=1$ ist $\mathfrak{r}$ im Körper $k(\sqrt[l]{\varkappa}, \zeta)$ das Product von l Primidealen; für den Charakter irgend eines dieser l Primideale erhalten wir den Wert

$$\left\{\frac{\varrho,\ \varkappa}{\mathfrak{q}}\right\}=\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}=1,$$

und damit ist der Hülfssatz 44 bewiesen.

Hülfssatz 45. Wenn $\mathfrak{q}, \bar{\mathfrak{q}}$ irgend zwei Primideale zweiter Art in $k(\zeta)$ sind, so ist stets $\left\{\frac{\mathfrak{q}}{\bar{\mathfrak{q}}}\right\}=\left\{\frac{\bar{\mathfrak{q}}}{\mathfrak{q}}\right\}$.

Beweis. Im Falle $\left\{\frac{\mathfrak{q}}{\bar{\mathfrak{q}}}\right\}=1$ folgt die Richtigkeit der Behauptung

unmittelbar aus Hülfssatz 44. Wir betrachten nunmehr den Fall $\left\{\frac{\mathfrak{q}}{\bar{\mathfrak{q}}}\right\} \neq 1$. Es seien $\varkappa$, $\bar{\varkappa}$ Primärzahlen bez. von $\mathfrak{q}$, $\bar{\mathfrak{q}}$; ferner seien $\mathfrak{q}'$, $\mathfrak{q}''$, ... die von $\mathfrak{q}$ verschiedenen, zu $\mathfrak{q}$ conjugirten Primideale und $\varkappa'$, $\varkappa''$, ... bez. die betreffenden zu $\varkappa$ conjugirten Primärzahlen von $\mathfrak{q}'$, $\mathfrak{q}''$, ...; andererseits seien $\bar{\mathfrak{q}}'$, $\bar{\mathfrak{q}}''$, ... die von $\bar{\mathfrak{q}}$ verschiedenen, zu $\bar{\mathfrak{q}}$ conjugirten Primideale und $\bar{\varkappa}'$, $\bar{\varkappa}''$, ... bez. die betreffenden zu $\bar{\varkappa}$ conjugirten Primärzahlen von $\bar{\mathfrak{q}}'$, $\bar{\mathfrak{q}}''$, ... Endlich sei q die durch $\mathfrak{q}$ teilbare rationale Primzahl; man hat dann $\varkappa\varkappa'\varkappa''\ldots = \varepsilon^l q^{hh^*}$, wo ε eine Einheit in $k(\zeta)$ ist. Nach Satz 152 (S. 426) giebt es ein Primideal $\mathfrak{r}$, für welches

$$(167.)\quad \left\{\frac{\varkappa}{\mathfrak{r}}\right\} = \zeta^*,\quad \left\{\frac{\varkappa'}{\mathfrak{r}}\right\} = 1,\quad \left\{\frac{\varkappa''}{\mathfrak{r}}\right\} = 1,\quad \ldots,$$

$$(168.)\quad \left\{\frac{\bar{\varkappa}}{\mathfrak{r}}\right\} = \zeta^*,\quad \left\{\frac{\bar{\varkappa}'}{\mathfrak{r}}\right\} = 1,\quad \left\{\frac{\bar{\varkappa}''}{\mathfrak{r}}\right\} = 1,\quad \ldots,$$

$$(169.)\quad \left\{\frac{\zeta}{\mathfrak{r}}\right\} = 1,\quad \left\{\frac{\varepsilon_1}{\mathfrak{r}}\right\} = 1,\quad \left\{\frac{\varepsilon_2}{\mathfrak{r}}\right\} = 1,\ \ldots,\ \left\{\frac{\varepsilon_{l^*}}{\mathfrak{r}}\right\} = 1$$

wird, wo ζ^* irgend eine von 1 verschiedene Einheitswurzel bedeutet, und wo $\varepsilon_1, \ldots, \varepsilon_{l^*}$ die l^* in § 166 bestimmten und dort mit $\varepsilon_1, \varepsilon_2', \ldots, \varepsilon_{l^*}^{(l^*-1)}$ bezeichneten Einheiten in $k(\zeta)$ sind. Aus (167.) folgt

$$\left\{\frac{\varkappa\varkappa'\varkappa''\ldots}{\mathfrak{r}}\right\} = \left\{\frac{q}{\mathfrak{r}}\right\} = \zeta^*,$$

und daher ist, wenn ϱ eine Primärzahl von $\mathfrak{r}$ bedeutet, nach Satz 140 (S. 369) auch

$$(170.)\qquad \left\{\frac{\varrho}{q}\right\} = \left\{\frac{\varrho}{\mathfrak{q}}\right\}\left\{\frac{\varrho}{\mathfrak{q}'}\right\}\left\{\frac{\varrho}{\mathfrak{q}''}\right\}\cdots = \zeta^*.$$

Andererseits ist wegen (167.) nach Hülfssatz 44

$$\left\{\frac{\varrho}{\mathfrak{q}'}\right\} = 1,\quad \left\{\frac{\varrho}{\mathfrak{q}''}\right\} = 1,\quad \ldots;$$

und daher folgt aus (170.) $\left\{\frac{\varrho}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} = \zeta^*$, es ist also

$$(171.)\qquad \left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} \neq 1.$$

In gleicher Weise leiten wir aus (168.) die Beziehung her:

$$(172.)\qquad \left\{\frac{\bar{\mathfrak{q}}}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{r}}{\bar{\mathfrak{q}}}\right\}^{\pm 1}.$$

Wir bestimmen nun die Potenz ϱ^e von ϱ so, dass $\left\{\frac{\varkappa\varrho^e}{\bar{\mathfrak{q}}}\right\} = 1$ wird, und betrachten dann den Kummer'schen Körper $k(\sqrt[l]{\varkappa\varrho^e}, \zeta)$. Da $\mathfrak{q}$ nach Voraussetzung und $\mathfrak{r}$ wegen (169.) Primideale zweiter Art sind, so folgt vermittelst des Hülfssatzes 43, dass die Relativdiscriminante dieses Körpers nur die beiden Primideale $\mathfrak{q}$, $\mathfrak{r}$ enthält. Nach Hülfssatz 35 (S. 470) giebt es daher in $k(\sqrt[l]{\varkappa\varrho^e}, \zeta)$ höchstens l Geschlechter. Das Primideal $\mathfrak{r}$ ist die $l$te Potenz eines Primideals $\mathfrak{R}$ in $k(\sqrt[l]{\varkappa\varrho^e}, \zeta)$. Die beiden Charaktere von $\mathfrak{R}$ in diesem Körper sind

$$\left\{\frac{\varrho,\ \varkappa\varrho^e}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\},\quad \left\{\frac{\varrho,\ \varkappa\varrho^e}{\mathfrak{r}}\right\} = \left\{\frac{\varkappa}{\mathfrak{r}}\right\}^{-1} = \left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}^{-1},$$

und hieraus ergeben sich die Charaktere von $\mathfrak{R}^2, \mathfrak{R}^3, \ldots, \mathfrak{R}^l$. Wegen (171.) bestimmen die l Ideale $\mathfrak{R}, \mathfrak{R}^2, \ldots, \mathfrak{R}^l$ l verschiedene Geschlechter, und wegen der nämlichen Formel (171.) ist zugleich für dieselben stets das Product ihrer beiden Charaktere gleich 1. Die letztere Thatsache gilt folglich für jedes beliebige Ideal in $k(\sqrt[l]{\varkappa\varrho^e}, \zeta)$. Da $\left\{\frac{\varkappa\varrho^e}{\bar{\mathfrak{q}}}\right\} = 1$ ist, so wird $\bar{\mathfrak{q}}$ in $k(\sqrt[l]{\varkappa\varrho^e}, \zeta)$ weiter zerlegbar; die Charaktere eines Primfactors von $\bar{\mathfrak{q}}$ sind

$$\left\{\frac{\bar{\varkappa},\ \varkappa\varrho^e}{\mathfrak{q}}\right\} = \left\{\frac{\bar{\varkappa}}{\mathfrak{q}}\right\},\quad \left\{\frac{\bar{\varkappa},\ \varkappa\varrho^e}{\mathfrak{r}}\right\} = \left\{\frac{\bar{\varkappa}}{\mathfrak{r}}\right\}^e,$$

und es ist daher das Product $\left\{\frac{\bar{\varkappa}}{\mathfrak{q}}\right\}\left\{\frac{\bar{\varkappa}}{\mathfrak{r}}\right\}^e = 1$. Da andererseits

$$\left\{\frac{\varkappa\varrho^e}{\bar{\mathfrak{q}}}\right\} = \left\{\frac{\mathfrak{q}}{\bar{\mathfrak{q}}}\right\}\left\{\frac{\mathfrak{r}}{\bar{\mathfrak{q}}}\right\}^e = 1$$

sein soll, so folgt unter Heranziehung von (172.) $\left\{\frac{\bar{\mathfrak{q}}}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\bar{\mathfrak{q}}}\right\}$.

Hülfssatz 46. Es sei $\mathfrak{p}$ ein Primideal der ersten Art und $\mathfrak{q}$ ein

Primideal der zweiten Art in $k(\zeta)$; wenn dann $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = 1$ ausfällt, so wird auch $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} = 1$.

Beweis. Es seien π, $\varkappa$ Primärzahlen bez. von $\mathfrak{p}$, $\mathfrak{q}$. Wir nehmen an, es wäre $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} \neq 1$. Nach Satz 152 (S. 426) giebt es ein von $\mathfrak{p}$ und $\mathfrak{q}$ verschiedenes Primideal $\mathfrak{r}$, für welches

$$(173.) \qquad \left\{\frac{\pi}{\mathfrak{r}}\right\} \neq 1, \quad \left\{\frac{\varkappa}{\mathfrak{r}}\right\} \neq 1,$$

$$(174.) \quad \left\{\frac{\zeta}{\mathfrak{r}}\right\} = 1, \quad \left\{\frac{\varepsilon_1}{\mathfrak{r}}\right\} = 1, \quad \ldots, \left\{\frac{\varepsilon_{l^*}}{\mathfrak{r}}\right\} = 1$$

ausfällt, wo $\varepsilon_1, \ldots, \varepsilon_{l^*}$ die in § 166 bestimmten und dort mit $\varepsilon_1, \ldots, \varepsilon_{l^*}^{(l^*-1)}$ bezeichneten Einheiten sind. Wegen (174.) ist $\mathfrak{r}$ ein Primideal zweiter Art. Bedeutet ϱ eine Primärzahl von $\mathfrak{r}$, so fällt $\left\{\frac{\varrho}{\mathfrak{p}}\right\} \neq 1$ aus; denn aus $\left\{\frac{\varrho}{\mathfrak{p}}\right\} = 1$ würde nach Hülfssatz 44 (S. 506) $\left\{\frac{\pi}{\mathfrak{r}}\right\} = 1$ folgen, was der ersten Gleichung in (173.) widerspräche. Wir können daher eine Potenz ϱ^e von ϱ bestimmen derart, dass $\left\{\frac{\varkappa\varrho^e}{\mathfrak{p}}\right\} = 1$ wird.

Da $\mathfrak{r}$, $\mathfrak{q}$ Primideale zweiter Art sind, so folgt mit Rücksicht auf Hülfssatz 43 (S. 502) nach Satz 148 (S. 393), dass die Relativdiscriminante des Körpers $k(\sqrt[l]{\varkappa\varrho^e}, \zeta)$ nur die beiden Primideale $\mathfrak{q}$, $\mathfrak{r}$ als Factoren enthält. Nun ist nach (173.) $\left\{\frac{\varkappa}{\mathfrak{r}}\right\} \neq 1$ und nach Hülfsatz 45 (S. 506)

$$\left\{\frac{\varkappa}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\},$$

und daraus folgt, wie im Beweise des Hülfssatzes 45, dass für jedes Ideal in $k(\sqrt[l]{\varkappa\varrho^e}, \zeta)$ das Product der beiden Charaktere gleich 1 sein muss. Wegen $\left\{\frac{\varkappa\varrho^e}{\mathfrak{p}}\right\} = 1$ wird $\mathfrak{p}$ in $k(\sqrt[l]{\varkappa\varrho^e}, \zeta)$ weiter zerlegbar; ein jeder Primfactor von $\mathfrak{p}$ besitzt als seine beiden Charaktere

$$\left\{\frac{\pi,\ \varkappa\varrho^e}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}, \quad \left\{\frac{\pi,\ \varkappa\varrho^e}{\mathfrak{r}}\right\} = \left\{\frac{\pi}{\mathfrak{r}}\right\}^e.$$

Da der erste Charakter nach Voraussetzung gleich 1 ist, so würde nach

dem eben Bewiesenen auch $\left\{\frac{\pi}{\mathfrak{r}}\right\} = 1$ folgen, was nach (173.) nicht zutrifft. Dadurch ist unsere Annahme $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} \neq 1$ widerlegt.

Hülfssatz 47. Wenn $\mathfrak{q}$ ein Primideal zweiter Art und $\mathfrak{p}$ ein Primideal erster Art ist, so folgt stets $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} = \left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}$.

Beweis. Wir verfahren genau wie im Beweise des Hülfssatzes 45, indem wir statt des Primideals $\bar{\mathfrak{q}}$ nunmehr das Primideal $\mathfrak{p}$ einsetzen und demgemäss im Verlauf des Beweises behufs Ableitung der (172.) entsprechenden Beziehung statt des Hülfssatzes 44 den Hülfssatz 46 heranziehen.

§ 169.

Ein Hülfssatz über das Product $\Pi'\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$, worin $\mathfrak{w}$ alle von $\mathfrak{l}$ verschiedenen Primideale durchläuft.

Wir sind nunmehr im Stande, den folgenden Hülfssatz abzuleiten:

Hülfssatz 48. Wenn ν, μ zu $\mathfrak{l}$ prime ganze Zahlen sind und überdies μ der $l$ten Potenz einer ganzen Zahl in $k(\zeta)$ nach $\mathfrak{l}^l$ congruent wird, so ist stets

$$\underset{(\mathfrak{w})}{\Pi'}\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = 1,$$

wo das Product über alle von $\mathfrak{l}$ verschiedenen Primideale $\mathfrak{w}$ in $k(\zeta)$ erstreckt werden soll.

Beweis. Unter der über μ gemachten Voraussetzung können wir offenbar μ gleich einem Product aus lauter Primärzahlen von Primidealen, dividirt durch die $l$te Potenz einer ganzen Zahl in $k(\zeta)$, setzen. Ist ν insbesondere gleich einer Primärzahl $\varkappa$ eines Primideals $\mathfrak{q}$ zweiter Art, so folgt alsdann die Richtigkeit der Behauptung sofort aus den Hülfssätzen 45 und 47, d. h. es ist unter der über μ gemachten Voraussetzung stets

$$(175.)\qquad \underset{(\mathfrak{w})}{\Pi'}\left\{\frac{\varkappa, \mu}{\mathfrak{w}}\right\} = 1.$$

Nunmehr betrachten wir den Kummer'schen Körper $k(\sqrt[l]{\mu}, \zeta)$. Wenn r die Anzahl der Charaktere bezeichnet, die das Geschlecht einer Klasse in diesem Körper bestimmen, so giebt es nach Hülfssatz 35

(S. 470) höchstens l^{r-1} Geschlechter in diesem Körper. Sind nun $\gamma_1, \ldots, \gamma_r$ irgend r solche $l$te Einheitswurzeln, deren Product gleich 1 ist, so können wir genau wie beim Beweise des Satzes 164 (S. 492) nachweisen, dass es stets Ideale in $k(\sqrt[l]{\mu}, \zeta)$ giebt, deren Charaktere mit $\gamma_1, \ldots, \gamma_r$ übereinstimmen. Dabei ist nur zu den Bedingungen (155.), (156.), denen das dort mit $\mathfrak{p}$ bezeichnete Primideal genügen soll, noch das Bedingungssystem

$$\left\{\frac{\zeta}{\mathfrak{p}}\right\} = 1, \quad \left\{\frac{\varepsilon_1}{\mathfrak{p}}\right\} = 1, \quad \ldots, \quad \left\{\frac{\varepsilon_{l^*}}{\mathfrak{p}}\right\} = 1$$

hinzuzunehmen, wo $\varepsilon_1, \ldots, \varepsilon_{l^*}$ die in § 166 bestimmten und dort mit $\varepsilon_1, \ldots, \varepsilon_{l^*}^{(l^*-1)}$ bezeichneten Einheiten sind. Auf diese Weise wird nämlich erreicht, dass $\mathfrak{p}$ obenein noch ein Primideal zweiter Art wird, und wegen dieses Umstandes dürfen wir mit Rücksicht auf die Hülfssätze 45 und 47 das Reciprocitätsgesetz in der nämlichen Weise anwenden, wie dies beim Beweise des Satzes 164 geschehen ist. Statt des dort benutzten Satzes 163 ziehen wir hier die Formel (175.) heran. Zugleich folgt, dass in $k(\sqrt[l]{\mu}, \zeta)$ wirklich l^{r-1} Geschlechter vorhanden sind, und damit zugleich, dass für jedes derselben das Product der r Charaktere stets gleich 1 sein muss. Diese Thatsache bringen wir nun zur Anwendung, um den Hülfssatz 48 für den Fall zu beweisen, dass ν eine Einheit ist, und weiter für den Fall, dass ν eine Primärzahl eines Primideals erster Art ist.

Es seien wiederum $\varepsilon_1, \ldots, \varepsilon_{l^*}$ die soeben erwähnten l^* Einheiten; ferner $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$, wie in § 149, die t in der Relativdiscriminante von $k(\sqrt[l]{\mu}, \zeta)$ aufgehenden verschiedenen Primideale, und es mögen darunter $\mathfrak{l}_t, \mathfrak{l}_{t-1}, \ldots, \mathfrak{l}_{r+1}$ wie in § 149 ausgewählt sein; ferner seien $\lambda_{r+1}, \ldots, \lambda_t$ Primärzahlen bez. von $\mathfrak{l}_{r+1}, \ldots, \mathfrak{l}_t$; endlich sei ξ eine beliebige Einheit in $k(\zeta)$. Nach Satz 152 (S. 426) giebt es ein Primideal $\mathfrak{q}$, für welches bei einem gewissen zu l primen Exponenten m

$$(176.)\quad \left\{\frac{\zeta}{\mathfrak{q}}\right\} = 1, \quad \left\{\frac{\varepsilon_1}{\mathfrak{q}}\right\} = 1, \quad \ldots, \quad \left\{\frac{\varepsilon_{l^*}}{\mathfrak{q}}\right\} = 1, \quad \left\{\frac{\mu}{\mathfrak{q}}\right\} = 1,$$

$$(177.)\quad \begin{cases} \left\{\dfrac{\lambda_{r+1}}{\mathfrak{q}}\right\} = \left\{\dfrac{\xi}{\mathfrak{l}_{r+1}}\right\}^m, \quad \left\{\dfrac{\lambda_{r+2}}{\mathfrak{q}}\right\} = \left\{\dfrac{\xi}{\mathfrak{l}_{r+2}}\right\}^m, \quad \ldots \\ \qquad\qquad \ldots, \quad \left\{\dfrac{\lambda_t}{\mathfrak{q}}\right\} = \left\{\dfrac{\xi}{\mathfrak{l}_t}\right\}^m \end{cases}$$

wird. Es sei $\varkappa$ eine Primärzahl von $\mathfrak{q}$. Wegen der Gleichung $\left\{\frac{\mu}{\mathfrak{q}}\right\}=1$ zerfällt $\mathfrak{q}$ im Körper $k(\sqrt[l]{\mu}, \zeta)$, und wegen der übrigen Gleichungen (176.) ist $\mathfrak{q}$ ein Primideal zweiter Art. Die r Charaktere eines Primfactors von $\mathfrak{q}$ haben, da, wie man aus (177.) und durch die Hülfssätze 45 und 47 erkennt,

$$(178.)\qquad \left\{\frac{\xi^{-m}\varkappa,\ \mu}{\mathfrak{l}_{r+1}}\right\}=1,\quad \ldots,\quad \left\{\frac{\xi^{-m}\varkappa,\ \mu}{\mathfrak{l}_t}\right\}=1$$

ist, folgende Werte:

$$\left\{\frac{\xi^{-m}\varkappa,\ \mu}{\mathfrak{l}_1}\right\},\quad \left\{\frac{\xi^{-m}\varkappa,\ \mu}{\mathfrak{l}_2}\right\},\quad \ldots,\quad \left\{\frac{\xi^{-m}\varkappa,\ \mu}{\mathfrak{l}_r}\right\}.$$

Nun muss nach dem oben Bewiesenen das Product derselben gleich 1 sein; dies liefert mit Rücksicht auf (178.) und auf die letzte Gleichung in (176.) die Beziehung

$$\mathop{\Pi'}_{(\mathfrak{w})}\left\{\frac{\xi^{-m}\varkappa,\ \mu}{\mathfrak{w}}\right\}=1,$$

wo das Product über alle von $\mathfrak{l}$ verschiedenen Primideale $\mathfrak{w}$ zu erstrecken ist; daraus folgt dann weiter mit Hülfe von (175.)

$$(179.)\qquad \mathop{\Pi'}_{(\mathfrak{w})}\left\{\frac{\xi^{-m},\ \mu}{\mathfrak{w}}\right\}=1,\quad \text{d. h.}\quad \mathop{\Pi'}_{(\mathfrak{w})}\left\{\frac{\xi,\ \mu}{\mathfrak{w}}\right\}=1;$$

der Hülfssatz 48 gilt also auch in dem Falle, dass ν eine beliebige Einheit in $k(\zeta)$ vorstellt.

Nunmehr sei $\mathfrak{p}$ irgend ein Primideal der ersten Art, welches die Bedingung $\left\{\frac{\mu}{\mathfrak{p}}\right\}=1$ erfüllt und folglich in $k(\sqrt[l]{\mu}, \zeta)$ zerlegbar ist. Die r Charaktere eines beliebigen Primfactors von $\mathfrak{p}$ sind, wenn π eine Primärzahl von $\mathfrak{p}$ und ξ eine geeignete Einheit in $k(\zeta)$ bedeutet,

$$\left\{\frac{\xi\pi,\ \mu}{\mathfrak{l}_1}\right\},\quad \left\{\frac{\xi\pi,\ \mu}{\mathfrak{l}_2}\right\},\quad \ldots,\quad \left\{\frac{\xi\pi,\ \mu}{\mathfrak{l}_r}\right\}.$$

Da das Product derselben gleich 1 sein muss, so folgt wie vorhin:

$$\mathop{\Pi'}_{(\mathfrak{w})}\left\{\frac{\xi\pi,\ \mu}{\mathfrak{w}}\right\}=1$$

und hieraus wegen (179.):

$$\mathop{\Pi'}_{(\mathfrak{w})}\left\{\frac{\pi,\ \mu}{\mathfrak{w}}\right\}=1.$$

Ist endlich $\mathfrak{p}$ ein solches, zu μ primes Primideal erster Art, für welches $\left\{\frac{\mu}{\mathfrak{p}}\right\} \neq 1$ ist, so bestimme man ein Primideal zweiter Art $\mathfrak{q}$ derart, dass $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} \neq 1$ ist; dann ist nach Hülfssatz 44 auch $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} \neq 1$. Bedeutet $\varkappa$ eine Primärzahl von $\mathfrak{q}$ und $\varkappa^e$ eine solche Potenz von $\varkappa$, dass $\left\{\frac{\mu\varkappa^e}{\mathfrak{p}}\right\} = 1$ wird, so ist nach dem soeben Bewiesenen

$$\underset{(\mathfrak{w})}{\Pi'}\left\{\frac{\pi,\ \mu\varkappa^e}{\mathfrak{w}}\right\} = 1,$$

und da auf Grund des Hülfssatzes 47 auch

$$\underset{(\mathfrak{w})}{\Pi'}\left\{\frac{\pi,\ \varkappa}{\mathfrak{w}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}^{-1}\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = 1$$

ausfällt, so folgt weiter

$$\underset{(\mathfrak{w})}{\Pi'}\left\{\frac{\pi,\ \mu}{\mathfrak{w}}\right\} = 1; \tag{180.}$$

der Hülfssatz 48 gilt also auch dann, wenn ν eine Primärzahl eines beliebigen Primideals erster Art ist. Aus (175.), (179.), (180.) folgt die allgemeine Gültigkeit des Hülfssatzes 48.

§ 170.

Das Symbol $\{\nu, \mu\}$ und das Reciprocitätsgesetz zwischen zwei beliebigen Primidealen.

Wir gelangen jetzt in überraschend einfacher Weise zu der am Anfang dieses Capitels in Aussicht gestellten neuen Begründung der Theorie des regulären Kummer'schen Körpers. Setzen wir, wenn ν und μ ganze Zahlen in $k(\zeta)$ bedeuten,

$$\{\nu,\ \mu\} = \left(\underset{(\mathfrak{w})}{\Pi'}\left\{\frac{\nu,\ \mu}{\mathfrak{w}}\right\}\right)^{-1}, \tag{181.}$$

wo das Product $\underset{(\mathfrak{w})}{\Pi}$ wiederum über alle von $\mathfrak{l}$ verschiedenen Primideale $\mathfrak{w}$ in $k(\zeta)$ zu erstrecken ist, so stellt das **Symbol** $\{\nu,\ \mu\}$ eine $l$te Einheitswurzel dar, die durch die Zahlen ν, μ völlig bestimmt ist, und es folgen aus (80.) (S. 411) sofort die Formeln

$$\left\{\begin{aligned} \{\nu_1\nu_2,\ \mu\} &= \{\nu_1,\ \mu\}\{\nu_2,\ \mu\}, \\ \{\nu,\ \mu_1\mu_2\} &= \{\nu,\ \mu_1\}\{\nu,\ \mu_2\}, \\ \{\nu,\ \mu\}\{\mu,\ \nu\} &= 1, \end{aligned}\right. \tag{182.}$$

in denen ν, ν_1, ν_2, μ, μ_1, μ_2 beliebige ganze Zahlen in $k(\zeta)$ bedeuten. Bezeichnet ferner r eine Primitivzahl nach l und $s = (\zeta : \zeta^r)$ die betreffende Substitution der Gruppe von $k(\zeta)$, so folgt

$$(183.) \qquad \{s\nu,\ s\mu\} = \{\nu,\ \mu\}^r.$$

Ferner ergiebt sich die Thatsache:

Hülfssatz 49. Wenn ν, μ zwei primäre Zahlen des Körpers $k(\zeta)$ sind, so hat das Symbol $\{\nu, \mu\}$ stets den Wert 1.

Beweis. Zunächst folgt, wenn a irgend eine ganze rationale, zu l und zu ν prime Zahl ist, mit Rücksicht auf Satz 140 (S. 369) die Gleichung

$$(184.) \qquad \{\nu,\ a\} = \left\{\frac{\nu}{a}\right\}^{-1} \left\{\frac{a}{\nu}\right\} = 1.$$

Da μ eine primäre Zahl sein soll, so ist $\mu . s^{\frac{l-1}{2}} \mu$ einer ganzen rationalen Zahl nach $\mathfrak{l}^{l-1}$ congruent. Infolgedessen können wir dann auch nach $\mathfrak{l}^l$ eine ganze rationale Zahl a bestimmen derart, dass die Congruenz

$$a . \mu . s^{\frac{l-1}{2}} \mu \equiv 1, \quad (\mathfrak{l}^l)$$

besteht, und ausserdem wieder a prim zu ν wählen. Nun ergiebt sich bei Anwendung des Hülfssatzes 48

$$\{\nu,\ a\}\{\nu,\ \mu\}\{\nu,\ s^{\frac{l-1}{2}} \mu\} = \{\nu, a . \mu . s^{\frac{l-1}{2}} \mu\} = 1,$$

und folglich wird wegen (184.) auch

$$\{\nu,\ \mu\}\{\nu,\ s^{\frac{l-1}{2}} \mu\} = 1.$$

Entsprechend beweisen wir

$$\{\nu,\ s^{\frac{l-1}{2}} \mu\}\{s^{\frac{l-1}{2}} \nu,\ s^{\frac{l-1}{2}} \mu\} = 1.$$

Aus Formel (183.) ergiebt sich ferner

$$\{\nu,\ \mu\}\{s^{\frac{l-1}{2}} \nu,\ s^{\frac{l-1}{2}} \mu\} = 1.$$

Die drei letzten Gleichungen zusammengenommen liefern

$$\{\nu,\ \mu\}^2 = 1, \quad \text{d. h.} \quad \{\nu,\ \mu\} = 1,$$

und damit ist der Hülfssatz 49 bewiesen.

Wählen wir insbesondere ν, μ als Primärzahlen von zwei beliebigen Primidealen $\mathfrak{p}$, $\mathfrak{q}$ in $k(\zeta)$, so ist die Aussage des Hülfssatzes 49 mit dem allgemeinen Reciprocitätsgesetze 161 (S. 471) für diese Primideale $\mathfrak{p}$, $\mathfrak{q}$ gleichbedeutend.

§ 171.

Uebereinstimmung des Symbols $\{\nu, \mu\}$ mit dem Symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$.

Wir schliessen aus Satz 151 (S. 420), wobei nur der Fall $\mathfrak{w} \neq \mathfrak{l}$ dieses Satzes zur Anwendung kommt, dass $\{\nu, \mu\}$ stets den Wert 1 besitzt, sobald ν die Relativnorm einer ganzen Zahl des Körpers $k(\sqrt[l]{\mu}, \zeta)$ ist; und endlich gelingt jetzt auch der Nachweis dafür, dass $\{\alpha, \mu\}$ stets den Wert 1 hat, so bald die ganze Zahl α Normenrest des Körpers $k(\sqrt[l]{\mu}, \zeta)$ nach $\mathfrak{l}$ ist. In der That, nehmen wir der Kürze wegen an, dass beide Zahlen α, μ zu $\mathfrak{l}$ prim sind, und setzen wir $\alpha \equiv N_k(A)$ nach $\mathfrak{l}^l$, wo $N_k(A)$ die Relativnorm einer ganzen Zahl A in $k(\sqrt[l]{\mu}, \zeta)$ bedeuten soll, so ist die Zahl $\alpha.(N_k(A))^{l-1}$ offenbar der $l$ten Potenz einer ganzen Zahl nach $\mathfrak{l}^l$ congruent; daher wird unter Benutzung der Formeln (182.) sowie mit Rücksicht auf die vorausgeschickten Bemerkungen und den Hülfssatz 48:

$$\{\alpha.(N_k(A))^{l-1}, \ \mu\} = \{\alpha, \ \mu\}\{N_k(A), \ \mu\}^{l-1} = \{\alpha, \ \mu\} = 1,$$

wie behauptet wurde. Wenn eine der Zahlen α, μ oder beide durch $\mathfrak{l}$ teilbar sind, so gelingt der Nachweis dieser Formel ebenfalls ohne Mühe vermöge der nämlichen Hülfsmittel.

Ist μ eine ganze, zu $\mathfrak{l}$ prime Zahl in $k(\zeta)$, so folgt aus (181.) leicht die Gleichung

$$\{\zeta, \ \mu\} = \zeta^{\frac{1-n(\mu)}{l}};$$

demnach erfüllt der Ausdruck $\{\nu, \mu\}$ sämtliche Forderungen, die für das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ am Schluss des § 133 aufgestellt worden sind; es ist somit, wenn wir die dort auf S. 423 unten angegebene Definition des Symbols $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ zu Grunde legen,

$$\{\nu, \ \mu\} = \left\{\frac{\nu, \ \mu}{\mathfrak{l}}\right\};$$

in dieser Gleichung erkennen wir dann den Satz 163 (S. 490) wieder.

Sind insbesondere die beiden Zahlen ν, μ zu $\mathfrak{l}$ prim und $\bar{\nu}$, $\bar{\mu}$

ganze Zahlen in $k(\zeta)$, die mit den ersteren durch die Congruenzen

$$\nu \equiv \bar{\nu}, \quad \mu \equiv \bar{\mu}, \quad (\mathfrak{l}^l)$$

verknüpft sind, so erhalten wir durch Benutzung des Hülfssatzes 48 leicht

$$\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\} = \left\{\frac{\bar{\nu},\ \bar{\mu}}{\mathfrak{l}}\right\}.$$

Hieraus und in Ansehung der Formeln (182.) entnehmen wir folgende Thatsache: Wenn die beiden Zahlen ν, μ zu $\mathfrak{l}$ prim sind und

$$\nu \equiv a^l (1+\lambda)^{n_1} (1+\lambda^2)^{n_2} \ldots (1+\lambda^{l-1})^{n_{l-1}}, \quad (\mathfrak{l}^l),$$

$$\mu \equiv b^l (1+\lambda)^{m_1} (1+\lambda^2)^{m_2} \ldots (1+\lambda^{l-1})^{m_{l-1}}, \quad (\mathfrak{l}^l)$$

gesetzt wird, wo a, b und die Exponenten

$$n_1, \quad n_2, \quad \ldots, \quad n_{l-1}; \quad m_1, \quad m_2, \quad \ldots, \quad m_{l-1}$$

ganze rationale Zahlen sind, so besteht eine Gleichung von der Gestalt

$$\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\} = \zeta^{L(n_1,\ \ldots,\ n_{l-1};\ m_1,\ \ldots,\ m_{l-1})};$$

dabei ist L eine homogene bilineare Function der beiden Reihen von Veränderlichen $n_1, \ldots, n_{l-1}; m_1, \ldots, m_{l-1}$, und die Coefficienten von L sind, ganze rationale Zahlen die nur von der Primzahl l abhängen, und die man bei gegebenem Werte der Primzahl l etwa durch besondere Annahmen der Zahlen ν, μ leicht berechnen kann.

Nachdem nun das Symbol $\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\}$ definirt und seine wichtigsten Eigenschaften abgeleitet worden sind, dürfen wir die in diesem Capitel bisher festgehaltene Einschränkung auf Kummer'sche Körper mit einer zu $\mathfrak{l}$ primen Relativdiscriminante fallen lassen; es gelangen dann, genau wie oben, die Sätze 164 (S. 492), 165 (S. 495), 166 (S. 495) und vor allem der Fundamentalsatz 167 (S. 496) zum Nachweise. Mit Hülfe dieses Satzes 167 und geeigneter Benutzung des Satzes 152 (S. 426) lässt sich dann auch zeigen, dass, wenn ν, μ zwei beliebige ganze Zahlen in $k(\zeta)$ mit der Eigenschaft $\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\} = 1$ sind und μ nicht gleich der $l$ten Potenz einer ganzen Zahl in $k(\zeta)$ ausfällt, die Zahl ν stets Normenrest des Kummer'schen Körpers $k(\sqrt[l]{\mu}, \zeta)$ nach $\mathfrak{l}$ sein muss. Damit ist dann der Satz 151 (S. 420) für den Fall $\mathfrak{w} = \mathfrak{l}$ nachträglich als richtig erkannt, und es folgt hieraus auch die Gültigkeit des

Satzes 150 (S. 402) für $\mathfrak{w} = \mathfrak{l}$. Bei der hier dargelegten Begründungsart der Theorie des Kummer'schen Körpers erscheinen also die Sätze 150 und 151 für $\mathfrak{w} = \mathfrak{l}$ im Gegensatz zu dem früheren Aufbau als die Schlusssteine des ganzen Gebäudes.

Capitel XXXVI.

Die Diophantische Gleichung $\alpha^m + \beta^m + \gamma^m = 0$.

§ 172.

Die Unmöglichkeit der Diophantischen Gleichung $\alpha^l + \beta^l + \gamma^l = 0$ für reguläre Primzahlexponenten l.

Fermat hat die Behauptung aufgestellt, dass die Gleichung

$$a^m + b^m + c^m = 0$$

in ganzen rationalen, von Null verschiedenen Zahlen a, b, c für keinen ganzzahligen Exponenten $m > 1$ lösbar ist. Wenngleich schon aus der Litteratur vor *Kummer* vereinzelte Resultate über diese Gleichung von *Fermat* bemerkenswert sind [*Abel*[1], *Cauchy*[1, 2], *Dirichlet*[1, 2, 3]] *Lamé*[1, 2, 3], *Lebesgue*[1, 2, 3]], so ist es doch erst *Kummer* auf Grund der Theorie der Ideale des regulären Kreiskörpers gelungen, den Beweis der *Fermat*'schen Behauptung für sehr umfassende Klassen von Exponenten m vollständig zu führen. Die wichtigste von *Kummer* bewiesene Thatsache ist die folgende:

Satz 168. Wenn l eine reguläre Primzahl bedeutet und α, β, γ irgend welche ganze Zahlen des Kreiskörpers der $l$ten Einheitswurzeln sind, von denen keine verschwindet, so besteht niemals die Gleichung

$$\alpha^l + \beta^l + \gamma^l = 0. \tag{185.}$$

[*Kummer*[1, 9, 11].]

Beweis. Es sei $\zeta = e^{\frac{2i\pi}{l}}$, $\lambda = 1 - \zeta$, $\mathfrak{l} = (\lambda)$. Wir nehmen im Gegensatz zu der Behauptung an, die Gleichung (185.) besässe eine Lösung in ganzen Zahlen α, β, γ des Körpers $k(\zeta)$, und unterscheiden dann die zwei Fälle, dass keine der drei ganzen Zahlen α, β, γ durch $\mathfrak{l}$ teilbar ist, oder dass mindestens eine unter ihnen durch $\mathfrak{l}$ teilbar ist.

Im ersten Falle sind jedenfalls für den Exponenten l die Werte 3 und 5 ausgeschlossen. In der That, für $l=3$ wäre jede der drei Zahlen α, β, $\gamma \equiv \pm 1$ nach $\mathfrak{l}$ und folglich jede der drei Potenzen α^3, β^3, $\gamma^3 \equiv \pm 1$ nach $\mathfrak{l}^3$; hieraus würde folgen, dass die Summe dieser drei Potenzen $\equiv \pm 1$ oder $\equiv \pm 3$ nach $\mathfrak{l}^3$ ausfiele, was mit dem Bestehen der Gleichung (185.) nicht verträglich ist. Auf einen ähnlichen Widerspruch gelangen wir für $l=5$, wenn wir berücksichtigen, dass in diesem Falle jede der drei Zahlen α, β, $\gamma \equiv \pm 1, \pm 2$ nach $\mathfrak{l}$ und folglich jede der drei Potenzen α^5, β^5, $\gamma^5 \equiv \pm 1, \pm 32$ nach $\mathfrak{l}^5$ sein müsste.

Es sei also $l \geqq 7$. Gilt die Gleichung (185.) für die drei Zahlen α, β, γ, so ist offenbar auch $\alpha^{*} + \beta^{*l} + \gamma^{*l} = 0$, wenn α^*, β^*, γ^* bezüglich die Producte von α, β, γ mit irgend welchen $l$ten Einheitswurzeln bedeuten. Wegen dieses Umstandes dürfen wir von vorn herein annehmen, dass die drei der Gleichung (185.) genügenden Zahlen α, β, γ semiprimär sind. Wir bringen nun die Gleichung (185.) in die Gestalt

$$(186.)\quad (\alpha+\beta)(\alpha+\zeta\beta)(\alpha+\zeta^2\beta)\dots(\alpha+\zeta^{l-1}\beta) = -\gamma^l.$$

Würden hier zwei der l Factoren linker Hand, z. B. $\alpha+\zeta^u\beta$ und $\alpha+\zeta^{u+g}\beta$, einen Factor gemein haben, so müsste dieser auch in $(\zeta^g-1)\alpha$ und in $(1-\zeta^g)\beta$ aufgehen, und da $\dfrac{1-\zeta^g}{1-\zeta}$ eine Einheit ist und $\mathfrak{l}$ nicht in γ aufgeht, so müsste dieser gemeinsame Factor notwendig ein gemeinsamer Factor der Zahlen α und β sein. Da jeder Primfactor, der nur in einem der l Factoren linker Hand von (186.) aufgeht, wegen eben dieser Gleichung offenbar zu einem durch l teilbaren Exponenten darin vorkommen muss, so folgt, dass die l Factoren der linken Seite von (186.) die folgende Zerlegung gestatten:

$$\begin{aligned}
\alpha+\beta &= \mathfrak{j}^l\mathfrak{a},\\
\alpha+\zeta\beta &= \mathfrak{j}_1\mathfrak{a},\\
\alpha+\zeta^2\beta &= \mathfrak{j}_2^l\mathfrak{a},\\
&\cdots\cdots\\
\alpha+\zeta^{l-1}\beta &= \mathfrak{j}_{l-1}^l\mathfrak{a};
\end{aligned}$$

darin bedeutet $\mathfrak{a}$ den grössten gemeinsamen Idealteiler der Zahlen α, β, und $\mathfrak{j}$, $\mathfrak{j}_1$, $\mathfrak{j}_2$, $\dots$, $\mathfrak{j}_{l-1}$ sind gewisse Ideale in $k(\zeta)$. Da insbesondere

$\alpha+\zeta^{l-1}\beta$ zu $\mathfrak{l}$ prim ist, so können wir eine $l$te Einheitswurzel ζ^* bestimmen derart, dass $\zeta^*(\alpha+\zeta^{l-1}\beta)$ semiprimär wird; wir setzen

$$\mu=\frac{\alpha}{\zeta^*(\alpha+\zeta^{l-1}\beta)},\quad \varrho=\frac{\beta}{\zeta^*(\alpha+\zeta^{l-1}\beta)}.$$

Es ergiebt sich dann

$$(187.)\quad \left\{\begin{aligned} \mu+\varrho &= \left(\frac{\mathfrak{j}}{\mathfrak{j}_{l-1}}\right)^l, \\ \mu+\zeta\varrho &= \left(\frac{\mathfrak{j}_1}{\mathfrak{j}_{l-1}}\right)^l, \\ &\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ \mu+\zeta^{l-2}\varrho &= \left(\frac{\mathfrak{j}_{l-2}}{\mathfrak{j}_{l-1}}\right)^l, \end{aligned}\right.$$

d. h. es ist

$$\left(\frac{\mathfrak{j}}{\mathfrak{j}_{l-1}}\right)^l\sim 1,\quad \left(\frac{\mathfrak{j}_1}{\mathfrak{j}_{l-1}}\right)^l\sim 1,\quad \ldots,\quad \left(\frac{\mathfrak{j}_{l-2}}{\mathfrak{j}_{l-1}}\right)^l\sim 1,$$

und ferner wird

$$(188.)\quad \mu+\zeta^{l-1}\varrho=\zeta^{*-1}.$$

Bedeutet h die Anzahl der Idealklassen in $k(\zeta)$, so ist andererseits

$$\left(\frac{\mathfrak{j}}{\mathfrak{j}_{l-1}}\right)^h\sim 1,\quad \left(\frac{\mathfrak{j}_1}{\mathfrak{j}_{l-1}}\right)^h\sim 1,\quad \ldots,\quad \left(\frac{\mathfrak{j}_{l-2}}{\mathfrak{j}_{l-1}}\right)^h\sim 1,$$

und da h zu l prim ist, so folgt hieraus weiter

$$\frac{\mathfrak{j}}{\mathfrak{j}_{l-1}}\sim 1,\quad \frac{\mathfrak{j}_1}{\mathfrak{j}_{l-1}}\sim 1,\quad \ldots,\quad \frac{\mathfrak{j}_{l-2}}{\mathfrak{j}_{l-1}}\sim 1.$$

Die Gleichungen (187.) können infolgedessen und mit Rücksicht auf Satz 127 (S. 336) in der Gestalt

$$(189.)\quad \mu+\zeta^u\varrho=\zeta^{e_u}\varepsilon_u\alpha_u^l,\qquad (u=0,1,2,\ldots,l-2)$$

geschrieben werden, wo die e_u gewisse ganzzahlige Exponenten, die ε_u geeignete reelle Einheiten des Kreiskörpers $k(\zeta)$ und die α_u gewisse ganze oder gebrochene Zahlen mit zu $\mathfrak{l}$ primen Zählern und Nennern in $k(\zeta)$ bedeuten. Da die $l$te Potenz der Zahl α_u jedesmal congruent einer gewissen ganzen rationalen Zahl a_u nach $\mathfrak{l}^l$ ist, so erhalten wir

aus den Gleichungen (189.) die Congruenzen

$$(190.)\qquad \mu+\zeta^u\varrho \equiv \zeta^{e_u}\varepsilon_u a_u, \quad (\mathfrak{l}^l), \qquad (u=0,1,2,\ldots,l-2).$$

Auf diese Congruenzen wenden wir die Substitution $(\zeta:\zeta^{-1})$ an und bezeichnen die bei dieser Substitution aus μ und ϱ hervorgehenden Zahlen mit μ' und ϱ'; dann entsteht

$$(191.)\qquad \mu'+\zeta^{-u}\varrho' \equiv \zeta^{-e_u}\varepsilon_u a_u, \quad (\mathfrak{l}^l), \qquad (u=0,1,2,\ldots,l-2).$$

Aus (190.) und (191.) folgt

$$(192.)\qquad \mu+\zeta^u\varrho \equiv \zeta^{2e_u}\mu'+\zeta^{2e_u-u}\varrho', \quad (\mathfrak{l}^l), \qquad (u=0,1,2,\ldots,l-2).$$

Setzen wir $\mu\equiv m$, $\varrho\equiv r$ nach $\mathfrak{l}^2$, wo m und r ganze rationale Zahlen bedeuten sollen, so folgt aus (192.)

$$(193.)\qquad m+\zeta^u r \equiv \zeta^{2e_u}m+\zeta^{2e_u-u}r, \quad (\mathfrak{l}^2),$$

und wegen der allgemeinen Beziehung $\zeta^g\equiv 1-g\lambda$ nach $\mathfrak{l}^2$ liefert (193.) die Congruenz:

$$2e_u(m+r)\equiv 2ru, \quad (l).$$

Andererseits folgt aus der Gleichung (188.) $m+r\equiv 1$ nach l, und daher haben wir

$$e_u\equiv ru, \quad (l), \qquad (u=0,1,2,\ldots,l-2).$$

Nehmen wir nun unter Berücksichtigung dieser Beziehung speciell die Congruenzen (192.) für $u=0,1,2,3$, so folgt aus diesen durch Elimination der Zahlen μ, ϱ, μ', ϱ' notwendig

$$\begin{vmatrix} 1, & 1, & 1, & 1 \\ 1, & \zeta, & \zeta^{2r}, & \zeta^{2r-1} \\ 1, & (\zeta)^2, & (\zeta^{2r})^2, & (\zeta^{2r-1})^2 \\ 1, & (\zeta)^3, & (\zeta^{2r})^3, & (\zeta^{2r-1})^3 \end{vmatrix} \equiv 0, \quad (\mathfrak{l}^l),$$

d. i.

$$(194.)\quad (1-\zeta)(1-\zeta^{2r})(1-\zeta^{2r-1})(\zeta-\zeta^{2r})(\zeta-\zeta^{2r-1})(\zeta^{2r}-\zeta^{2r-1})\equiv 0, \ (\mathfrak{l}^l).$$

Hier ist auf der linken Seite keiner der Factoren gleich 0, denn sonst müsste entweder $r\equiv 0$ oder $r\equiv 1$ oder $r\equiv\frac{1}{2}$ nach l sein. Wäre $r\equiv 0$ nach l, so würde $\beta\equiv 0$ nach $\mathfrak{l}$ folgen; wäre $r\equiv 1$ nach l, so würde $\varrho\equiv 1$ nach $\mathfrak{l}$, d. h. $\beta\equiv\alpha+\beta$ oder $\alpha\equiv 0$ nach $\mathfrak{l}$ folgen;

beides läuft unserer Annahme über die Zahlen α, β, γ zuwider. Wäre $r \equiv \frac{1}{2}$ nach l, so würde $\varrho \equiv \frac{1}{2}$ nach $\mathfrak{l}$, d. h. $2\beta \equiv \alpha + \beta$ oder $\alpha \equiv \beta$ nach $\mathfrak{l}$ folgen. Da aber α, β, γ in der Gleichung (185.) symmetrisch auftreten, so würde die gleiche Schlussweise auch zu der Congruenz $\alpha \equiv \gamma$ nach $\mathfrak{l}$ führen, und dann wäre $\alpha^l + \beta^l + \gamma^l \equiv 3\alpha \equiv 0$, d. h. $\alpha \equiv 0$ nach $\mathfrak{l}$, was wiederum unserer Annahme über α, β, γ widerspricht. Jeder Factor auf der linken Seite der Congruenz (194.) ist demnach durch $\mathfrak{l}$, aber nicht durch $\mathfrak{l}^2$ teilbar, daher ist mit Rücksicht auf die Annahme $l \geqq 7$ diese Congruenz (194.) unmöglich.

Wir nehmen nunmehr zweitens an, es sei in der Gleichung (185.) eine der drei Zahlen α, β, γ, etwa γ, durch $\mathfrak{l}$ teilbar, und zwar gehe in γ genau die $m$te Potenz von $\mathfrak{l}$ auf. Wird dann γ durch $\lambda^m \delta$ ersetzt, so dass δ eine zu $\mathfrak{l}$ prime ganze Zahl in $k(\zeta)$ bedeutet, so ist die aus (185.) entstehende Gleichung von der Gestalt

$$\alpha^l + \beta^l = \varepsilon \lambda^{lm} \delta^l; \tag{195.}$$

hierin ist $\varepsilon = -1$. Es soll jetzt gezeigt werden, dass überhaupt eine Gleichung von dieser Gestalt (195.) nicht möglich ist, wenn in derselben α, β, δ zu $\mathfrak{l}$ prime ganze Zahlen und ε irgend eine Einheit des Kreiskörpers $k(\zeta)$ sein sollen. Zu dem Zwecke nehmen wir wiederum die Zahlen α, β semiprimär an und bedenken dann zunächst, dass α^l, β^l ganzen rationalen Zahlen nach $\mathfrak{l}^{l+1}$ congruent werden und daher wegen (195.) auch $\varepsilon \lambda^{ml} \delta^l$ einer ganzen rationalen Zahl nach $\mathfrak{l}^{l+1}$ congruent sein muss; infolgedessen ist notwendig $m > 1$. Ferner erkennen wir durch eine ähnliche Ueberlegung wie in dem vorher behandelten Falle und in Berücksichtigung des Umstandes, dass $\alpha + \beta$ semiprimär ist, die Gültigkeit der folgenden Gleichungen:

$$\left\{\begin{aligned} \alpha + \beta &= \lambda^{l(m-1)+1} \mathfrak{j}^l \mathfrak{a}, \\ \alpha + \zeta\beta &= \lambda \mathfrak{j}_1^l \mathfrak{a}, \\ &\cdots\cdots\cdots \\ \alpha + \zeta^{l-1}\beta &= \lambda \mathfrak{j}_{l-1}^l \mathfrak{a}, \end{aligned}\right. \tag{196.}$$

wo $\mathfrak{j}, \mathfrak{j}_1, \ldots, \mathfrak{j}_{l-1}, \mathfrak{a}$ zu $\mathfrak{l}$ prime Ideale in $k(\zeta)$ sind. Ist insbesondere $l = 3$, so fällt die Klassenanzahl h des Körpers $k(\zeta)$ gleich 1 aus, und es ist daher jedes Ideal in $k(\zeta)$ ein Hauptideal. Setzen wir in diesem Falle $\mathfrak{a} = (\varkappa)$, wo $\varkappa$ eine ganze Zahl in $k(\zeta)$ bedeute, und dann

$$\mu = \frac{\alpha}{\varkappa}, \quad \varrho = \frac{\beta}{\varkappa},$$

so gehen die Gleichungen (196.) über in

$$(197.)\quad \begin{cases} \mu+\varrho = \lambda^{3(m-1)+1}\mathfrak{j}^l, \\ \mu+\zeta\varrho = \lambda\mathfrak{j}_1^l, \\ \mu+\zeta^2\varrho = \lambda\mathfrak{j}_2^l. \end{cases}$$

Im Falle $l > 3$ bilden wir die Zahlen

$$\mu = \frac{\alpha\lambda}{\alpha+\zeta^{l-1}\beta}, \quad \varrho = \frac{\beta\lambda}{\alpha+\zeta^{l-1}\beta};$$

dieselben lassen sich auch in der Gestalt von Brüchen schreiben, deren Zähler und Nenner zu $\mathfrak{l}$ prim sind. Aus den drei ersten und der letzten der Gleichungen (196.) entnehmen wir die Gleichungen

$$(198.)\quad \begin{cases} \mu+\varrho = \lambda^{l(m-1)+1}\left(\dfrac{\mathfrak{j}}{\mathfrak{j}_{l-1}}\right)^l, \\ \mu+\zeta\varrho = \lambda\left(\dfrac{\mathfrak{j}_1}{\mathfrak{j}_{l-1}}\right)^l, \\ \mu+\zeta^2\varrho = \lambda\left(\dfrac{\mathfrak{j}_2}{\mathfrak{j}_{l-1}}\right)^l. \end{cases}$$

Wie in dem zuerst behandelten Falle schliessen wir hieraus wiederum

$$\frac{\mathfrak{j}}{\mathfrak{j}_{l-1}} \sim 1, \quad \frac{\mathfrak{j}_1}{\mathfrak{j}_{l-1}} \sim 1, \quad \frac{\mathfrak{j}_2}{\mathfrak{j}_{l-1}} \sim 1,$$

und infolgedessen können wir die Gleichungen (198.) in der Gestalt

$$(199.)\quad \begin{cases} \mu+\varrho = \dfrac{\varepsilon^*\lambda^{l(m-1)+1}\gamma^{*l}}{\nu}, \\ \mu+\zeta\varrho = \dfrac{\lambda\alpha^{*l}}{\nu}, \\ \mu+\zeta^2\varrho = \dfrac{\varepsilon\lambda\beta^{*l}}{\nu}, \end{cases}$$

schreiben, so dass ν, α^*, β^*, γ^* ganze, zu $\mathfrak{l}$ prime Zahlen und ε und ε^* Einheiten in $k(\zeta)$ bedeuten. Wegen (197.) besteht ein Gleichungssystem wie (199.) auch für $l=3$. Durch Elimination von μ, ϱ folgt daher

für $l=3$ sowie für $l>3$ eine Gleichung von der Gestalt:

$$\alpha^{*l}+\eta\beta^{*l} = \eta^*\lambda^{l(m-1)}\gamma^{*l}, \tag{200.}$$

wo η und η^* $\left(=-\frac{(1-\zeta)}{(1-\zeta^2)}\,\varepsilon \text{ und } =\frac{\zeta(1-\zeta)}{(1-\zeta^2)}\,\varepsilon^*\right)$ Einheiten in $k(\zeta)$ sind. Da α^{*l}, β^{*l}, ganzen rationalen Zahlen nach $\mathfrak{l}^l$ congruent sind und, wie vorhin bewiesen, $m>1$ ausfällt, so folgt in Anbetracht dieser Gleichung (200.), dass auch η einer ganzen rationalen Zahl nach $\mathfrak{l}^l$ congruent sein muss, und daher ist nach Satz 156 (S. 439) η die $l$te Potenz einer Einheit in $k(\zeta)$. Schreiben wir nun in der Gleichung (200.) $\beta^*\eta^{-\frac{1}{l}}$ an Stelle von β^*, so nimmt diese Gleichung die Gestalt von (195.) an, nur dass der Exponent m jetzt um 1 kleiner geworden ist. Die wiederholte Anwendung des nämlichen Verfahrens auf die Gleichung (200.) würde notwendig zu einer Gleichung von der Form (195.) mit $m=1$ und dadurch auf einen Widerspruch führen. Damit ist der Satz 168 vollständig bewiesen.

§ 173.

Weitere Untersuchungen über die Unmöglichkeit der Diophantischen Gleichung $\alpha^m+\beta^m+\gamma^m=0$.

Der Beweis der Unlösbarkeit der Gleichung $\alpha^l+\beta^l+\gamma^l=0$ in ganzen Zahlen α, β, γ des Kreiskörpers der $l$ten Einheitswurzeln ist von *Kummer* noch in dem Falle erbracht worden, dass l eine Primzahl ist, die in der Klassenanzahl h des Kreiskörpers $k\left(e^{\frac{2i\pi}{l}}\right)$ zur ersten, aber nicht zu einer höheren Potenz aufgeht [*Kummer*[16]]. Der Bemerkung auf S. 437 zufolge ist somit die *Fermat*'sche Behauptung insbesondere für jeden Exponenten $m\leqq 100$ als richtig erkannt. Die Aufgabe, die *Fermat*'sche Behauptung allgemein als richtig zu erweisen, harrt jedoch noch ihrer Lösung.

Es bleibt noch übrig, die Gleichung $\alpha^m+\beta^m+\gamma^m=0$ für den Fall zu behandeln, dass der Exponent m eine Potenz von 2 ist. Die Gleichung $a^2+b^2=c^2$ besitzt bekanntlich unendlich viele Lösungen in ganzen rationalen Zahlen a, b, c. Weiter gilt jedoch der Satz:

Satz 169. Wenn α, β, γ ganze Zahlen des durch $i=\sqrt{-1}$ bestimmten quadratischen Körpers sind, von denen keine verschwindet, so gilt niemals die Gleichung

$$\alpha^4+\beta^4 = \gamma^2. \tag{201.}$$

Beweis. Wir nehmen im Gegenteil an, dass es drei solche ganze Zahlen α, β, γ gebe, welche diese Gleichung erfüllen. Es werde $\lambda = 1+i$ und $\mathfrak{l} = (\lambda)$ gesetzt. Zunächst sehen wir dann leicht ein, dass notwendig eine der beiden Zahlen α, β durch λ teilbar sein muss. In der That, nehmen wir an, dass α und β prim zu λ wären, und berücksichtigen wir, dass eine zu λ prime ganze Zahl in $k(i)$ stets $\equiv 1$ oder i nach $\mathfrak{l}^2$, ihre zweite Potenz dann $\equiv \pm 1$ nach $\mathfrak{l}^4$ und ihre vierte notwendig $\equiv 1$ nach $\mathfrak{l}^6$ sein muss, so folgt $\alpha^4 + \beta^4 \equiv 2$ nach $\mathfrak{l}^6$. Hiernach müsste γ notwendig durch $\mathfrak{l}$ und durch keine höhere Potenz von $\mathfrak{l}$ teilbar sein. Setzen wir aber dementsprechend $\gamma = \lambda + \lambda^2\gamma'$, wo γ' wiederum eine ganze Zahl in $k(i)$ bedeute, so finden wir $\gamma^2 \equiv 2i$ nach $\mathfrak{l}^4$ und daher stets $\gamma^2 \not\equiv \alpha^4 + \beta^4$ nach $\mathfrak{l}^4$, womit unsere Annahme widerlegt ist. Der Fall, dass beide Zahlen α und β durch $\mathfrak{l}$ teilbar sind, kann offenbar sofort ausgeschlossen werden, da dann γ durch $\mathfrak{l}^2$ teilbar und somit das Fortheben der Potenz λ^4 auf beiden Seiten der Gleichung (201.) möglich wäre.

Es bleibt also nur die Annahme übrig, dass die eine der Zahlen α, β, etwa die Zahl α, durch $\mathfrak{l}$ teilbar, die Zahlen β und γ dann aber zu $\mathfrak{l}$ prim sind. Wir setzen demgemäss $\alpha = \lambda^m \alpha^*$, wo α^* eine zu λ prime Zahl bedeute, und legen dann unserer Betrachtung sogleich die allgemeinere Gleichung

$$(202.)\qquad \beta^4 - \gamma^2 = \varepsilon \lambda^{4m} \alpha^{*4}$$

zu Grunde, wo ε eine beliebige Einheit in $k(i)$ bedeute. Wir entnehmen aus dieser Gleichung (202.), indem wir nötigenfalls γ mit $-\gamma$ vertauschen, zwei Gleichungen von der Gestalt:

$$(203.)\qquad \begin{cases} \beta^2 + \gamma = \eta \lambda^{4m-2} \alpha'^4, \\ \beta^2 - \gamma = \vartheta \lambda^2 \quad \beta'^4, \end{cases}$$

wobei η, ϑ Einheiten und α', β' ganze, zu $\mathfrak{l}$ prime Zahlen in $k(i)$ bedeuten. Wenn man die beiden Gleichungen (203.) addirt und das Resultat durch $\vartheta\lambda^2$ dividirt, so entsteht eine Gleichung

$$(204.)\qquad \beta'^4 - \vartheta' \beta^2 = \eta' \lambda^{4m-4} \alpha'^4,$$

wo ϑ', η' Einheiten in $k(i)$ sind. Im Falle $m = 1$ wäre diese Gleichung sicher unmöglich, weil die Zahlen β', ϑ', β, η', α' sämtlich $\equiv 1$ nach $\mathfrak{l}$ ausfallen. Es ist daher notwendig $m > 1$. Dann aber folgt aus dieser Gleichung (204.), wenn sie als Congruenz nach $\mathfrak{l}^2$ aufgefasst wird, zunächst $\vartheta' \equiv 1$ nach $\mathfrak{l}^2$; es ist daher $\vartheta' = \pm 1$. Setzen wir,

je nachdem hier das positive oder das negative Vorzeichen gilt, $\beta = \gamma'$ bez. $\beta = i\gamma'$, so nimmt die Gleichung (204.) die Gestalt der Gleichung (202.) an, nur dass jetzt m einen um 1 kleineren Wert hat. Die gehörige Wiederholung des angegebenen Verfahrens führt auf einen Widerspruch.

Aus der *Fermat*'schen Behauptung für den Fall $l = 3$ lässt sich sofort die Thatsache ableiten, dass es keine andere cubische Gleichung mit rationalen Coefficienten giebt, deren Discriminante gleich 1 ist, ausser den zwei folgenden:

$$x^3 - x \pm \tfrac{1}{3} = 0$$

und denjenigen, die durch die Transformation $x = x' + a$, wo a eine rationale Zahl ist, aus jenen Gleichungen hervorgehen. [*Kronecker*[8].]

Die allgemeine *Fermat*'sche Behauptung lässt sich nach *Hurwitz* in der Fassung aussprechen, dass der Ausdruck $\sqrt[m]{1 - x^m}$ für eine positive, echt gebrochene rationale Zahl x und einen ganzen rationalen Exponenten $m > 2$ stets eine irrationale Zahl darstellt.

Verzeichnis der Litteratur.

Die hinter jeder einzelnen Abhandlung in eckiger Klammer beigefügten Zahlen bezeichnen die Seiten des Berichtes, auf denen die Abhandlung genannt ist.

N. H. Abel.

1. Extraits de quelques lettres à Holmboe. Werke. Bd. 2 S. 254. [517]

F. Arndt.

1. Bemerkungen über die Verwandlung der irrationalen Quadratwurzel in einen Kettenbruch. Journ. für Math. Bd. 31. 1846. [285]

P. Bachmann.

1. Zur Theorie der complexen Zahlen. Journ. für Math. Bd. 67. 1867. [321, 390]
2. Die Lehre von der Kreisteilung und ihre Beziehungen zur Zahlentheorie. Leipzig 1872. [334]
3. Ergänzung einer Untersuchung von Dirichlet. Math. Ann. Bd. 16. 1880. [321]

H. Berkenbusch.

1. Ueber die aus den 8ten Wurzeln der Einheit entspringenden Zahlen. Inauguraldissertation. Marburg 1891. [364]

A. L. Cauchy.

1. Mémoire sur la théorie des nombres. Comptes rendus. 1840. [386]
2. Mémoire sur diverses propositions relatives à la théorie des nombres. (Drei Noten.) Comptes rendus. 1847. [517]

A. Cayley.

1. Tables des formes quadratiques binaires pour les déterminants négatifs dépuis $D = -1$ jusqu'à $D = -100$, pour les déterminants positifs non

carrés depuis $D=2$ jusqu'à $D=99$ et pour les treize déterminants négatifs irréguliers qui se trouvent dans le premier millier. Werke. Bd. 5. S. 141. 1862. [285]

R. Dedekind.

1. Vorlesungen über Zahlentheorie von P. G. Lejeune Dirichlet. Auflage II bis IV. Braunschweig 1871—1894. Supplement XI [177, 179, 181, 184, 191, 192, 214, 224, 226, 227, 232, 234, 236, 245, 280, 284, 315, 322, 326, 377, 381] und Supplement VII [334].
2. Sur la théorie des nombres entiers algébriques. Paris 1877. Abdruck aus Bull. des sciences math. et astron. s. 1 t. XI und s. 2 t. I. [177]
3. Ueber die Anzahl der Idealklassen in den verschiedenen Ordnungen eines endlichen Körpers. Braunschweig 1877. [238, 244, 245, 246, 322]
4. Ueber den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen. Abh. der K. Ges. der Wiss. zu Göttingen 1878. [203]
5. Sur la théorie des nombres complexes idéaux. Comptes rendus Bd. 90. 1880. [333]
6. Ueber die Discriminanten endlicher Körper. Abh. der K. Ges. der Wiss. zu Göttingen 1882. [193, 195, 239, 245]
7. Ueber einen arithmetischen Satz von Gauss. Mitteilungen der deutschen math. Ges. zu Prag 1892 und: Ueber die Begründung der Idealtheorie. Nachr. d. K. Ges. der Wiss. zu Göttingen. 1895. [184]
8. Zur Theorie der Ideale. Nachr. der K. Ges. der Wiss. zu Göttingen 1894. [267]
9. Ueber eine Erweiterung des Symbols $(\mathfrak{a}, \mathfrak{b})$ in der Theorie der Moduln. Nachr. der K. Ges. der Wiss. zu Göttingen. 1895. [245]

G. Lejeune Dirichlet.

1. Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré. Werke. Bd. 1. S. 1. 1825. [517]
2. Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré. Werke. Bd. 1. S. 21. 1825, 1828. [517]
3. Démonstration du théorème de Fermat pour le cas des 14ièmes puissances. Werke. Bd. 1. S. 189. 1832. [517]
4. Einige neue Sätze über unbestimmte Gleichungen. Werke. Bd. 1. S. 219. 1834. [285]
5. Beweis eines Satzes über die arithmetische Progression. Werke. Bd. 1. S. 307. 1837. [381]
6. Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält. Werke. Bd. 1. S. 313. 1837. [381]
7. Sur la manière de résoudre l'équation $t^2-pu^2=1$ au moyen des fonctions circulaires. Werke. Bd. 1. S. 343. [226, 384]

8. Sur l'usage des séries infinies dans la théorie des nombres. Werke. Bd. 1. S. 357. 1838. [226, 310, 318]
9. Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres. Werke. Bd. 1. S. 411. 1839, 1840. [310, 318]
10. Untersuchungen über die Theorie der complexen Zahlen. Werke. Bd. 1. S. 503. 1841. [321]
11. Untersuchungen über die Theorie der complexen Zahlen. Werke. Bd. 1. S. 509. 1841. [321]
12. Recherches sur les formes quadratiques à coefficients et à indéterminées complexes. Werke. Bd. 1. S. 533. 1842. [321]
13. Sur la théorie des nombres. Werke. Bd. 1. S. 619. 1840. [214]
14. Einige Resultate von Untersuchungen über eine Klasse homogener Functionen des dritten und der höheren Grade. Werke. Bd. 1. S. 625. 1841. [214]
15. Sur un théorème relatif aux séries. Journ für Math. Bd. 53. 1857. [231]
16. Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen. Werke. Bd. 1. S. 633. 1842 und: Zur Theorie der complexen Einheiten. Werke. Bd. 1. S. 639. 1846. [214]

G. Eisenstein.

1. Ueber eine neue Gattung zahlentheoretischer Functionen. Bericht der K. Akad. der Wiss. zu Berlin. 1850. [490]
2. Beweis der allgemeinsten Reciprocitätsgesetze zwischen reellen und complexen Zahlen. Bericht der K. Akad. der Wiss. zu Berlin. 1850. [369]
3. Ueber die Anzahl der quadratischen Formen, welche in der Theorie der complexen Zahlen zu einer reellen Determinante gehören. Journ. für Math. Bd. 27. 1844. [321]
4. Beiträge zur Kreisteilung. Journ. für Math. Bd. 27. 1844 [386]
5. Beweis des Reciprocitätsgesetzes für die cubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahlen. Journ. für Math. Bd. 27. 1844. [490]
6. Ueber die Anzahl der quadratischen Formen in den verschiedenen complexen Theorien. Journ. für Math. Bd. 27. 1844. [321]
7. Nachtrag zum cubischen Reciprocitätssatze für die aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahlen. Kriterien des cubischen Charakters der Zahl 3 und ihrer Teiler. Journ. für Math. Bd. 28. 1844. [490]
8. Loi de reciprocité. Nouvelle démonstration du théorème fondamental sur les résidus quadratiques dans la théorie des nombres complexes. Démonstration du théorème fondamental sur les résidus biquadratiques qui comprend comme cas particulier le théorème fondamental. Journ. für Math. Bd. 28. 1844. [490]
9. Einfacher Beweis und Verallgemeinerung des Fundamentaltheorems für die biquadratischen Reste. Journ. für Math. Bd. 28. 1844. [490]

10. Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln, welche der Kreisteilung ihre Entstehung verdanken. Journ. für Math. Bd. 28 und 29. 1844, 1845. [390]
11. Zur Theorie der quadratischen Zerfällung der Primzahlen $8n+3$, $7n+2$ und $7n+4$. Jorn. für Math. Bd. 37. 1848. [387]
12. Ueber ein einfaches Mittel zur Auffindung der höheren Reciprocitätsgesetze und der mit ihnen zu verbindenden Ergänzungssätze. Journ. für Math. Bd. 39. 1850. [490]

G. Frobenius.

1. Ueber Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe. Berichte der K. Akad. der Wiss. zu Berlin 1896 [537].

L. Fuchs.

1. Ueber die Perioden, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist. Journ. für Math. Bd. 61. 1862. [364]
2. Ueber die aus Einheitswurzeln gebildeten complexen Zahlen von periodischem Verhalten, insbesondere die Bestimmung der Klassenanzahl derselben. Journ. für Math. Bd. 65. 1864. [364].

C. F. Gauss.

1. Disquisitiones arithmeticae. 1801. Werke. Bd. 1. [285, 293]
2. Summatio quarundam serierum singularium. Werke. Bd. 2. S. 11. [388]
3. Theoria residuorum biquadraticorum, commentatio prima et secunda. Werke. Bd. 2 S. 65 und 93. [490]

J. A. Gmeiner.

1. Die Ergänzungssätze zum bicubischen Reciprocitätsgesetze. Ber. der K. Akad. der Wiss. zu Wien. 1891. [490]
2. Das allgemeine bicubische Reciprocitätsgesetz. Ber. der Akad. der Wiss. zu Wien. 1892. [490]
3. Die bicubische Reciprocität zwischen einer reellen und einer zweigliedrigen regulären Zahl. Monatshefte für Math. und Phys. Bd. 3. 1892. [490]

K. Hensel.

1. Arithmetische Untersuchungen über Discriminanten und ihre ausserwesentlichen Teiler. Inaugural-Dissert. Berlin 1884. [202, 203]
2. Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor. Journ. für Math. Bd. 101 und 103. 1887 und 1888. [202, 203]
3. Ueber Gattungen, welche durch Composition aus zwei anderen Gattungen entstehen. Journ. für Math. Bd. 105. 1889. [267]
4. Untersuchung der Fundamentalgleichung einer Gattung für eine reelle Primzahl als Modul und Bestimmung der Teiler ihrer Discriminante. Journ. für Math. Bd. 113. 1894. [195, 200]

5. Arithmetische Untersuchungen über die gemeinsamen ausserwesentlichen Discriminantenteiler einer Gattung. Journ. für Math. Bd. 113. 1894. [202, 203]

Ch. Hermite.

1. Sur la théorie des formes quadratiques ternaires indéfinies. Journ. für Math. Bd. 47. 1854. [212]
2. Extrait d'une lettre de M. Ch. Hermite à M. Borchardt sur le nombre limité d'irrationalités aux quelles se réduisent les racines des équations à coefficients entiers complexes d'un degré et d'un discriminant donnés. Journ. für Math. Bd. 53. 1857. [212]

D. Hilbert.

1. Zwei neue Beweise für die Zerlegbarkeit der Zahlen eines Körpers in Primideale. Jahresber. der Deutschen Mathematiker-Vereinigung. Bd. 3. 1893. [188, 247]
2. Ueber die Zerlegung der Ideale eines Zahlenkörpers in Primideale. Math. Ann. Bd. 44. 1894. [188, 247, 249]
3. Grundzüge einer Theorie des Galois'schen Zahlkörpers. Nachr. der K. Ges. der Wiss. zu Göttingen. 1894. [205, 250]
4. Ueber den Dirichlet'schen biquadratischen Zahlkörper. Math. Ann. Bd. 45. 1894. [321, 322]
5. Ein neuer Beweis des Kronecker'schen Fundamentalsatzes über Abel'sche Zahlkörper. Nachr. der K. Ges. der Wiss. zu Göttingen. 1896. [339]

A. Hurwitz.

1. Ueber die Theorie der Ideale. Nachr. der K. Ges. der Wiss. zu Göttingen. 1894. [184]
2. Ueber einen Fundamentalsatz der arithmetischen Theorie der algebraischen Grössen. Nachr. der K. Ges. der Wiss. zu Göttingen. 1895. [184]
3. Zur Theorie der algebraischen Zahlen. Nachr. der K. Ges. der Wiss. zu Göttingen. 1895. [188]
4. Die unimodularen Substitutionen in einem algebraischen Zahlenkörper. Nachr. der K. Ges. der Wiss. zu Göttingen. 1895. [225]

C. G. J. Jacobi.

1. De residuis cubicis commentatio numerosa. Werke. Bd. 6. S. 233. 1827. [386, 490]
2. Observatio arithmetica de numero classium divisorum quadraticorum formae y^2+Az^2 designante A numerum primum formae $4n+3$. Werke. Bd. 6. S. 240. 1832. [364, 386]
3. Ueber die Kreistheilung und ihre Anwendung auf die Zahlentheorie. Werke. Bd. 6. S. 254. 1837. [386]
4. Ueber die complexen Primzahlen, welche in der Theorie der Reste der 5ten, 8ten und 12ten Potenzen zu betrachten sind. Werke. Bd. 6. S. 275. 1839. [386, 490]

L. Kronecker.

1. De unitatibus complexis. Dissertatio inauguralis. Berolini 1845. Werke. Bd. 1. S. 5. 1845. [272]
2. Ueber die algebraisch auflösbaren Gleichungen. Ber. der K. Akad. der Wiss. zu Berlin. 1853. [339]
3. Mémoire sur les facteurs irréductibles de l'expression x^n-1. Werke. Bd. 1. S. 75. 1854. [333]
4. Sur une formule de Gauss. Journ. de Math. 1856. [388]
5. Démonstration d'une théorème de M. Kummer. Werke. Bd. 1. S. 93 1856. [429]
6. Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten. Werke. Bd. 1. S. 103. 1857. [221]
7. Ueber complexe Einheiten. Werke. Bd. 1. S. 109. 1857. [336]
8. Ueber cubische Gleichungen mit rationalen Coefficienten. Werke. Bd. 1. S. 119. 1859. [525]
9. Ueber die Klassenanzahl der aus Wurzeln der Einheit gebildeten complexen Zahlen. Werke. Bd. 1. S. 123. 1863. [376]
10. Ueber den Gebrauch der Dirichlet'schen Methoden in der Theorie der quadratischen Formen. Ber. der K. Akad. der Wiss. zu Berlin. 1864. [310]
11. Auseinandersetzung einiger Eigenschaften der Klassenanzahl idealer complexer Zahlen. Werke. Bd. 1. S. 271. 1870. [232, 377]
12. Bemerkungen über Reuschle's Tafeln complexer Primzahlen. Ber. der K. Akad. der Wiss. zu Berlin. 1875. [383]
13. Ueber Abel'sche Gleichungen. Ber. der K. Akad. der Wiss. zu Berlin. 1877. [339]
14. Ueber die Irreductibilität von Gleichungen. Ber. der K. Akad. der Wiss. zu Berlin. 1880. [263, 265]
15. Ueber die Potenzreste gewisser complexer Zahlen. Ber. der K. Akad. der Wiss. zu Berlin. 1880. [384]
16. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. Journ. für Math. Bd. 92. 1882. [177, 179, 181, 186, 195, 200, 203, 224]
17. Zur Theorie der Abel'schen Gleichungen. Bemerkungen zum vorangehenden Aufsatz des Herrn Schwering. Journ. für Math. Bd. 93. 1882. [364]
18. Sur les unités complexes. (Drei Noten.) Comptes rendus. Bd. 96. 1883, vergl. auch J. Molk: Sur les unités complexes. Bull. des sciences math. et astron. 1883. [214]
19. Zur Theorie der Formen höherer Stufen. Ber. der K. Akad. der Wiss. zu Berlin. 1883. [184]
20. Additions au mémoire sur les unités complexes. Comptes rendus. Bd. 99. 1884. [214]
21. Ein Satz über Discriminanten-Formen. Journ. für Math. Bd. 100. 1886. [333]

E. Kummer.

1. De aequatione $x^{2\lambda}+y^{2\lambda}=z^{2\lambda}$ per numeros integros resolvenda. Journ. für Math. Bd. 17. 1837. [517]
2. Eine Aufgabe, betreffend die Theorie der cubischen Reste. Journ. für Math. Bd. 23. 1842. [364]
3. Ueber die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreisteilung entstehen. Journ. für Math. Bd. 30. 1846. [364]
4. De residuis cubicis disquisitiones nonnullae analyticae. Journ. für Math. Bd. 32. 1846. [364]
5. Zur Theorie der complexen Zahlen. Journ. für Math. Bd. 35. 1847. [182]
6. Ueber die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren. Journ. für Math. Bd. 35. 1847. [271, 358, 364]
7. Bestimmung der Anzahl nicht aequivalenter Klassen für die aus λten Wurzeln der Einheit gebildeten complexen Zahlen und die idealen Factoren derselben. Journ. für Math. Bd. 40. 1850. [377, 378]
8. Zwei besondere Untersuchungen über die Klassenanzahl und über die Einheiten der aus λten Wurzeln der Einheit gebildeten complexen Zahlen. Journ. für Math. Bd. 40. 1850. [429, 435, 439]
9. Allgemeiner Beweis des Fermat'schen Satzes, dass die Gleichung $x^\lambda+y^\lambda=z^\lambda$ durch ganze Zahlen lösbar ist, für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahlen sind und in den Zählern der ersten $\frac{1}{2}(\lambda-3)$ Bernoulli'schen Zahlen als Factoren nicht vorkommen. Journ. für Math. Bd. 40. 1850. [517]
10. Ueber allgemeine Reciprocitätsgesetze für beliebig hohe Potenzreste. Ber. der K. Akad. der Wiss. zu Berlin. 1850. [365, 471]
11. Mémoire sur la théorie des nombres complexes composés de racines de l'unité et des nombres entiers. Journ. de Math. Bd. 16. 1851. [358, 364, 377, 383, 437, 517]
12. Ueber die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen. Journ. für Math. Bd. 44. 1851. [412, 432, 441, 471]
13. Ueber die Irregularität der Determinanten. Ber. der K. Akad. der Wiss. zu Berlin. 1853. [364]
14. Ueber eine besondere Art aus complexen Einheiten gebildeter Ausdrücke. Journ. für Math. Bd. 50. 1854. [277]
15. Theorie der idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n=1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist. Abh. der K. Akad. der Wiss. zu Berlin. 1856. [333]
16. Einige Sätze über die aus den Wurzeln der Gleichung $\alpha^\lambda=1$ gebildeten complexen Zahlen für den Fall, dass die Klassenanzahl durch λ teilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes. Abh. der K. Akad. der Wiss. zu Berlin. 1857. [523]
17. Ueber die den Gauss'schen Perioden der Kreisteilung entsprechenden Congruenzwurzeln. Journ. für Math. Bd. 53. 1856. [364]

18. Ueber die allgemeinen Reciprocitätsgesetze der Potenzreste. Ber. der K. Akad. der Wiss. zu Berlin. 1858. [471]
19. Ueber die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen. Journ. für Math. Bd. 56. 1858. [471]
20. Ueber die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist. Abh. der K. Akad. der Wiss. zu Berlin. 1859. [277, 414, 416, 418, 425, 471, 494]
21. Zwei neue Beweise der allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist. Abh. der K. Akad. der Wiss. zu Berlin. 1861. abgedruckt im Journ. für Math. Bd. 100. [277, 471]
22. Ueber die Klassenanzahl der aus $n$ten Einheitswurzeln gebildeten complexen Zahlen. Ber. der K. Akad. der Wiss. zu Berlin. 1861. [376]
23. Ueber die Klassenanzahl der aus zusammengesetzten Einheitswurzeln gebildeten idealen complexen Zahlen. Ber. der K. Akad. der Wiss. zu Berlin. 1863. [376]
24. Ueber die einfachste Darstellung der aus Einheitswurzeln gebildeten complexen Zahlen, welche durch Multiplication mit Einheiten bewirkt werden kann. Bericht der K. Akad. der Wiss. zu Berlin. 1870. [383]
25. Ueber eine Eigenschaft der Einheiten der aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten complexen Zahlen und über den zweiten Factor der Klassenzahl. Ber. der K. Akad. der Wiss. zu Berlin. 1870. [377]
26. Ueber diejenigen Primzahlen λ, für welche die Klassenzahl der aus λten Einheitswurzeln gebildeten complexen Zahlen durch λ teilbar ist. Ber. der K. Akad. der Wiss. zu Berlin. 1874. [437]

J. L. Lagrange.

1. Sur la solution des problèmes indéterminés du second degré. Werke. Bd. 2. S. 375. 1868. [538]

G. Lamé.

1. Mémoire d'analyse indéterminée démontrant que l'équation $x^7+y^7=z^7$ est impossible en nombres entiers. Journ. de Math. 1840. [517]
2. Mémoire sur la résolution, en nombres complexes, de l'équation
$$A^5+B^5+C^5 = 0.$$
Journ. de Math. 1847. [517]
3. Mémoire sur la résolution, en nombres complexes, de l'équation
$$A^n+B^n+C^n = 0.$$
Journ. de Math. 1847. [517]

V. A. Lebesgue.

1. Démonstration de l'impossibilité de résoudre l'équation $x^7+y^7+z^7=0$ en nombres entiers. Journ. de Math. 1840. [517]
2. Addition à la note sur l'équation $x^7+y^7+z^7=0$. Journ. de Math. 1840. [517]
3. Théorèmes nouveaux sur l'équation indéterminée $x^5+y^5=az^5$. Journ. de Math. 1843. [517]

A. Legendre.

1. Essai sur la théorie des nombres. 1798. [285]

F. Mertens.

1. Ueber einen algebraischen Satz. Ber. der K. Akad. der Wiss. zu Wien. 1892. [184]

C. Minnigerode.

1. Ueber die Verteilung der quadratischen Formen mit complexen Coefficienten und Veränderlichen in Geschlechter. Nachr. der K. Ges. der Wiss. zu Göttingen. 1873. [321]

H. Minkowski.

1. Ueber die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen. Journ. für Math. Bd. 107. 1891. [211, 213, 224]
2. Théorèmes arithmétiques. Extrait d'une lettre à M. Hermite. Comptes rendus. Bd. 92. 1891. [211]
3. Geometrie der Zahlen. Leipzig 1896. [210, 211, 212, 213, 214, 221, 224]
4. Généralisation de la théorie des fractions continues. Ann. de l'école normale. 1896. [222]

C. G. Reuschle.

1. Tafeln complexer Primzahlen, welche aus Wurzeln der Einheit gebildet sind. Berlin 1875. [383]

E. Schering.

1. Zahlentheoretische Bemerkung. Auszug aus einem Brief an Herrn Kronecker. Journ. für Math. Bd. 100. 1887.
2. Die Fundamentalklassen der zusammensetzbaren arithmetischen Formen. Abh. der K. Ges. der Wiss. zu Göttingen. 1869. [232]

K. Schwering.

1. Zur Theorie der arithmetischen Functionen, welche von Jacobi $\psi(\alpha)$ genannt werden. Journ. für Math. Bd. 93. 1882. [364]
2. Untersuchung über die fünften Potenzreste und die aus fünften Einheitswurzeln gebildeten ganzen Zahlen. Zeitschrift für Math. und Phys. Bd. 27. 1882. [364]
3. Ueber gewisse trinomische complexe Zahlen. Acta Math. Bd. 10. 1887. [364]
4. Eine Eigenschaft der Primzahl 107. Acta Math. Bd. 11. 1887. [364]

J. A. Serret.

1. Handbuch der höheren Algebra. Deutsch von G. Wertheim. Bd. 2. Teil 3. Leipzig 1879. [195]

H. Smith.

1. Report on the theory of numbers. Werke. [364]

L. Stickelberger.

1. Ueber eine Verallgemeinerung der Kreisteilung. Math. Ann. Bd. 37. 1890. [387]

F. Tano.

1. Sur quelques théorèmes de Dirichlet. Journ. für Math. Bd. 105. [285]

H. Weber.

1. Theorie der Abel'schen Zahlkörper. Acta Math. Bd. 8 und 9. 1886 und 1887. [339, 376]
2. Ueber Abel'sche Zahlkörper dritten und vierten Grades. Sitzungsber. der Ges. zur Förderung der Naturw. zu Marburg. 1892. [390]
3. Zahlentheoretische Untersuchungen aus dem Gebiete der elliptischen Functionen. Nachr. der K. Ges. der Wiss. zu Göttingen. 1893. (Drei Mitteilungen.)
4. Lehrbuch der Algebra. Bd. 2. Braunschweig 1896. [318, 333, 376, 390]

P. Wolfskehl.

1. Beweis, dass der zweite Factor der Klassenanzahl für die aus den elften und dreizehnten Einheitswurzeln gebildeten Zahlen gleich eins ist. Journ. für Math. Bd. 99. 1885. [364].

Druckfehler, Berichtigungen und Zusätze.

S. 177. Z. 3 v. u. Statt „diese“ lies: „eine solche“.

S. 180. Z. 14. Statt „bestimmende Zahl“ lies: „bestimmende ganze Zahl“.

S. 182. Z. 5. Füge ein „[*Kummer* 5, 6]“.

S. 185. Z. 11. Man hat nämlich den Hülfssatz 2 auf diejenigen zwei Functionen der einen Veränderlichen x anzuwenden, welche aus F und R entstehen, wenn man darin

$$u_1 = x,\quad u_2 = x^{m+1},\quad u_3 = x^{(m+1)^2},\quad \ldots,\quad u_r = x^{(m+1)^{r-1}}$$

einsetzt.

S. 192. Z. 9. Füge hinzu: „vorausgesetzt, dass $\mathfrak{a}$ und $\mathfrak{b}$ zu einander prim sind“.

S. 200. Z. 7—5 v. u. Inwiefern Ideale eines Körpers k zugleich auch als Ideale eines höheren Körpers aufgefasst werden können, wird auf S. 204 Z. 12—19 auseinandergesetzt. Vgl. überdies den hier folgenden Zusatz zu S. 204.

S. 204. Z. 12—19. Dass wir berechtigt sind, unter den angegebenen Umständen $(\alpha_1, \ldots, \alpha_s)$ zugleich als ein Ideal in k und in K anzusehen, lehrt der folgende Satz: Wenn $\alpha_1, \ldots, \alpha_s$ und $\alpha_1^*, \ldots, \alpha_{s^*}^*$ ganze Zahlen in k sind, so dass in K die beiden Ideale $\mathfrak{J} = (\alpha_1, \ldots, \alpha_s)$ und $\mathfrak{J}^* = (\alpha_1^*, \ldots, \alpha_{s^*}^*)$ mit einander übereinstimmen, so stimmen auch in k die beiden Ideale $\mathfrak{j} = (\alpha_1, \ldots, \alpha_s)$ und $\mathfrak{j}^* = (\alpha_1^*, \ldots, \alpha_{s^*}^*)$ mit einander überein. In der That, wegen der Voraussetzung gilt, wenn α^* eine der Zahlen $\alpha_1^*, \ldots, \alpha_{s^*}^*$ bedeutet, eine Gleichung von der Gestalt $\alpha^* = A_1\alpha_1 + \cdots + A_s\alpha_s$, wo $A_1, \ldots, A_s$ gewisse ganze Zahlen in K sind. Wenn wir nun von beiden Seiten dieser Gleichung die Relativnorm bilden, so erkennen wir, dass im Körper k die Zahl α^{*r} durch $\mathfrak{j}^r$ teilbar sein muss; infolgedessen ist in k auch α^* durch $\mathfrak{j}$ und daher auch $\mathfrak{j}^*$ durch $\mathfrak{j}$ teilbar. Da in gleicher Weise das Umgekehrte gezeigt werden kann, so haben wir notwendig in k die Gleichung $\mathfrak{j} = \mathfrak{j}^*$.

S. 238. Z. 12—13. Statt: „in welchem $\iota_1, \ldots, \iota_m$ die Basis eines Ringideals bilden“ lies: „in welchem, wenn A eine geeignet gewählte ganze

rationale Zahl bedeutet, die Producte $A\iota_1, A\iota_2, \ldots, A\iota_m$ die Basis eines Ringideals bilden". Zum Beweise dieses Satzes 60 vergleiche den Beweis zu Satz 61.

S. 241. Z. 8 v. u. Statt „$\frac{H_1}{\Theta_1}, \ldots, \frac{H_m}{\Theta_1}$" lies „$\frac{H_1}{H}, \ldots, \frac{H_m}{H}$".

S. 241. Z. 7 v. u. ist das erste Mal „$\mathfrak{m}$" zu streichen.

S. 243. Z. 8 v. u. Statt: „$\mathfrak{j} = (\alpha_1, \ldots, \alpha_s)$ ist folglich zu $\mathfrak{f}$ prim" lies: „$\mathfrak{j}^* = (\alpha_1, \ldots, \alpha_s)$ ist folglich zu $\mathfrak{f}$ prim. Da $\mathfrak{j}^*$ durch $\mathfrak{j}$ teilbar ist und überdies in dem Product $\mathfrak{f}\mathfrak{j}$ aufgeht, so ergiebt sich daraus $\mathfrak{j}^* = \mathfrak{j}$; d. h. $\mathfrak{j}_r$ erweist sich als ein reguläres Ringideal, dem das Körperideal $\mathfrak{j}$ zugeordnet ist. Damit ist der Satz 64 bewiesen."

S. 258. Die sämtlichen in der Tabelle vorkommenden Gradzahlen und Exponenten haben für jedes in p aufgehende Primideal des Körpers K die gleichen Werte wie für $\mathfrak{P}$ und sind daher durch die Primzahl p allein völlig bestimmt.

S. 264. Für den Fall, dass die Gruppe der zur Bestimmung des Körpers k dienenden Gleichungen die symmetrische ist, lässt sich bereits aus den Bemerkungen *Kronecker*'s die Existenz der Dichtigkeiten $\Delta_0, \Delta_1, \ldots, \Delta_m$ entnehmen; für einen beliebigen Körper k hat *Frobenius* die Existenz dieser Dichtigkeiten bewiesen und zugleich ihre Werte bestimmt; sie sind rationale Zahlen, welche in einfacher Weise von der Gruppe der den Körper k bestimmenden Gleichungen abhängen. [*Frobenius* [1]].

S. 267. Z. 13 v. u. Statt „$\prod_{i,l} \mathfrak{P}_{il}^{e_i}$" lies „$\prod_{i,l} \mathfrak{J}_{il}^{e_i}$".

S. 267. Z. 12 v. u. Statt „$\mathfrak{P}_{il}$ dasjenige Primideal" lies „$\mathfrak{J}_{il}$ dasjenige Ideal".

S. 267. Nach Z. 11 v. u. füge die Worte hinzu: „Die Ideale $\mathfrak{J}_l$ sind nicht notwendig Primideale in K."

S. 273. Z. 2. Statt F_{r-1} lies F_{r+1}.

S. 279. Z. 9 v. u. Statt 90 lies 94.

S. 291. Am Schluss des § 64 füge hinzu:

Aus den Formeln (a'), (a''), (b'), (b'') in Satz 98 lässt sich folgende Thatsache ableiten:

Wenn man ein vollständiges System zu w primer und nach w^e incongruenter Zahlen ins Auge fasst, wo $e \geqq 1$ und im Falle $w = 2$ sogar $e > 2$ sei, so sind entweder alle diese Zahlen Normenreste des quadratischen Körpers $k(\sqrt{m})$ nach w oder nur die Hälfte, jenachdem w zu der Discriminante von $k(\sqrt{m})$ prim ist oder nicht.

S. 297. Z. 5. Hier fehlt der Nachweis, dass, wenn $\left(\frac{q}{q'}\right) = +1$ ist, notwendig $\left(\frac{q'}{q}\right) = -1$ sein muss. Das Reciprocitätsgesetz für zwei rationale Primzahlen q, q', die beide $\equiv 3$ nach 4 sind, folgt am einfachsten, wenn wir den quadratischen Körper $k(\sqrt{qq'})$ betrachten. Da wegen $\left(\frac{-1, qq'}{q}\right) = -1$ die Norm der Grundeinheiten ε dieses

Körpers jedenfalls $=+1$ sein muss, so giebt es nach Satz 90 eine ganze Zahl α in $k(\sqrt{qq'})$ von der Beschaffenheit, dass $\varepsilon=\alpha^{1-s}=\frac{\alpha}{s\alpha}$ wird, wo $s\alpha$ die zu α conjugirte Zahl bedeutet, und hieraus schliessen wir leicht, dass das in q enthaltene ambige Primideal $\mathfrak{q}$ notwendig ein Hauptideal sein muss. Folglich ist bei geeigneter Wahl des Vorzeichens gleichzeitig

$$\left(\frac{\pm q,\, qq'}{q}\right)=+1 \quad \text{und} \quad \left(\frac{\pm q,\, qq'}{q'}\right)=+1;$$

es ist daher in jedem Falle

$$\left(\frac{q,\, qq'}{q}\right)=\left(\frac{q,\, qq'}{q'}\right),$$

d. h. mit Rücksicht auf Formel (c') in Satz 98

$$-\left(\frac{q'}{q}\right)=\left(\frac{q}{q'}\right).$$

S. 299. Die Kriterien für die Auflösbarkeit der quadratischen ternären Diophantischen Gleichung sind zuerst von *Lagrange* gefunden worden [*Lagrange* [1]].

S. 299. Z. 10 v. u. statt „negativ" lies „positiv".

S. 333. Z. 9—25. Zum Beweise des Satzes 125 nehmen wir der Kürze wegen $m=l_1^{h_1}l_2^{h_2}$ an und bezeichnen dann die Kreiskörper der $l_1^{h_1}$ten, $l_2^{h_2}$ten Einheitswurzeln bez. mit $k^{(1)}$, $k^{(2)}$. Ferner sei p eine von l_1, l_2 verschiedene rationale Primzahl und $\mathfrak{p}^{(1)}$, $\mathfrak{p}^{(2)}$ seien je ein idealer Primfactor von p bez. in den Körpern $k^{(1)}$, $k^{(2)}$; wir bezeichnen in $k^{(1)}$, $k^{(2)}$ die Zerlegungskörper der Primideale $\mathfrak{p}^{(1)}$, $\mathfrak{p}^{(2)}$ bez. mit $k_z^{(1)}$, $k_z^{(2)}$. Es seien f_1, f_2 die kleinsten Exponenten, für welche $p^{f_1}\equiv 1$ nach $l_1^{h_1}$ bez. $p^{f_2}\equiv 1$ nach $l_2^{h_2}$ ausfällt, und es möge

$$l_1^{h_1-1}(l_1-1)=e_1f_1,\quad l_2^{h_2-1}(l_2-1)=e_2f_2$$

gesetzt werden: dann sind e_1, e_2 bez. die Grade der Körper $k_z^{(1)}$, $k_z^{(2)}$ und f_1, f_2 der Relativgrad von $k^{(1)}$ in Bezug auf $k_z^{(1)}$ bez. der Relativgrad von $k^{(2)}$ in Bezug auf $k_z^{(2)}$. Nach Satz 88 (vgl. die oben zu S. 267 angegebenen Verbesserungen) zerfällt die rationale Primzahl p in dem aus $k_z^{(1)}$, $k_z^{(2)}$ zusammengesetzten Körper $k_z^{(1,2)}$ in e_1e_2 Ideale; diese sind daher sämtlich Primideale ersten Grades in $k_z^{(1,2)}$. Wir betrachten unter diesen insbesondere das Primideal $\mathfrak{p}=(\mathfrak{p}^{(1)},\mathfrak{p}^{(2)})$ und bezeichnen mit $\mathfrak{P}$ einen Primfactor von $\mathfrak{p}$ in dem aus $k^{(1)}$, $k^{(2)}$ zusammengesetzten Körper k; es sei k_z der Zerlegungskörper des Primideals $\mathfrak{P}$ in k. Es folgt zunächst aus der Definition der Zerlegungskörper, dass $k_z^{(1,2)}$ entweder mit k_z übereinstimmen oder in k_z als Unterkörper enthalten sein muss. Die Relativgruppe des aus $k^{(1)}$, $k_z^{(2)}$ zusammengesetzten Körpers in Bezug auf $k_z^{(1,2)}$ ist cyklisch vom Grade f_1; die Relativgruppe des aus

$k_z^{(1)}$, $k^{(2)}$ zusammengesetzten Körpers in Bezug auf $k_z^{(1,2)}$ ist cyklisch vom Grade f_2. Wir entnehmen hieraus, dass, wenn f das kleinste gemeinsame Vielfache der Zahlen f_1, f_2 bedeutet, die Relativgruppe von k in Bezug auf $k_z^{(1,2)}$ keine cyklische Untergruppe von höherem als dem $f$ten Grade enthalten kann. Da k als Trägheitskörper des Primideals $\mathfrak{P}$ eine cyklische Relativgruppe in Bezug auf k_z besitzen muss und der Körper k_z den Körper $k_z^{(1,2)}$ enthält, so folgt, dass jene cyklische Relativgruppe von k in Bezug auf k_z höchstens den Grad f hat.

Andererseits stellen wir folgende Betrachtungen an. Die beiden Körper $k^{(1)}$ und k_z haben den Körper $k_z^{(1)}$, aber keinen Körper höheren Grades als gemeinsamen Unterkörper, da sonst $\mathfrak{p}^{(1)}$ in $k^{(1)}$ noch weiter zerlegbar sein müsste. Desgleichen haben die beiden Körper $k^{(2)}$ und k_z den Körper $k_z^{(2)}$ zum grössten gemeinsamen Unterkörper. Wir legen nun $k_z^{(1,2)}$ als Rationalitätsbereich zu Grunde; es ist dann k_z ein solcher Relativkörper in Bezug auf $k_z^{(1,2)}$, der weder mit $k^{(1)}$, noch mit $k^{(2)}$ einen Relativkörper in Bezug auf $k_z^{(1,2)}$ gemein hat. Hieraus schliessen wir ohne Mühe, dass k_z höchstens vom Relativgrade $\frac{f_1 f_2}{f}$ in Bezug auf $k_z^{(1,2)}$ sein kann. Der Körper k_z ist daher höchstens vom Grade $\frac{e_1 f_1 e_2 f_2}{f}$, d. h. die Relativgruppe von k in Bezug auf k_z hat mindestens den Grad f. Dies zusammen mit der oben bewiesenen Thatsache zeigt, dass der Grad der Relativgruppe von k in Bezug auf k_z gleich f sein muss, womit sich für den gegenwärtig betrachteten besonderen Fall die Aussage des Satzes 125 deckt.

S. 346. Z. 6 v. u. u. s. f. Wenn in einem beliebigen Körper k ein Ideal $\mathfrak{j}$ und zwei gebrochene Zahlen α, β vorgelegt sind, so soll die Congruenz $\alpha \equiv \beta$ nach $\mathfrak{j}$ besagen, dass es in k eine zu $\mathfrak{j}$ prime Zahl μ giebt, für welche $\mu\alpha$, $\mu\beta$ ganze Zahlen in k werden und überdies die Congruenz $\mu\alpha \equiv \mu\beta$ nach $\mathfrak{j}$ gilt.

S. 367. Zeile 3—6. Statt β setze überall $\mathfrak{b}$.

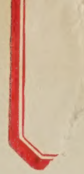
S. 367. Zeile 3. Statt „eine ganze Zahl oder ein beliebiges Ideal“ setze „ein beliebiges zu $\mathfrak{l}$ primes Ideal“.

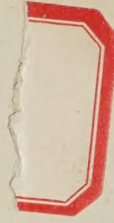
Verzeichnis der Sätze und Hülfssätze.

Die Sätze mit fettgedruckten Nummern sind im Text durch cursiven Druck ausgezeichnet.

Verzeichnis der Begriffsnamen.

Die den Begriffsnamen beigefügte Zahl bezeichnet diejenige Seite des Berichtes, auf welcher derselbe zum ersten Mal gebraucht wird. Auf dieser Seite ist der Name fett gedruckt und der Begriff erklärt.





Chiouby